OMCeOCampobasso
Ordine Provinciale dei Medici-Chirurghi e degli Odontoiatri

Determina Presidenziale n. 2 del 19/06/2025

OGGETTO: Adozione del Manuale di Gestione dei flussi documentali dell'Ordine dei Medici Chirurghi e degli Odontoiatri della Provincia di Campobasso – Versione Ed. 1/2025

Il Presidente dell'OMCeO della Provincia di Campobasso, Dr. Giuseppe De Gregorio,

PREMESSO che il 30 giugno 2025 risulta essere il termine ultimo per adempiere alla pubblicazione del "Manuale di gestione documentale", come da comunicazione pervenuta dalla FNOMCeO tramite nota PEC con Prot. N E-2025-0001124 del 09/06/2025;

PREMESSO che per tale incarico è stato nominato Responsabile della gestione documentale, come stabilito dal Piano Triennale per l'informatica nelle PA 2024-2026, il Funzionario Amministrativo Dott.ssa Maria, Giuliana Zicchillo, come persona in possesso di idonei requisiti professionali o di professionalità tecnico-archivistica, con responsabilità dei compiti ai sensi dell'Art. 4 del D.P.C.M. del 3 dicembre 2013 – "*Regole tecniche per il protocollo informatico*…"

VISTO il D. Lgs. 82/2005 "*Codice dell'Amministrazione Digitale*" e s.m.i.;

VISTO il D.P.R. 445/2000 "*Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa*";

CONSIDERATO che, con Deliberazione N. 64 del Consiglio Direttivo del 09/06/2025 sono stati approvati: l'istituzione del "Servizio Archivistico dell'Ordine", l'individuazione del Responsabile del servizio e la predisposizione del *Manuale di Gestione* dei flussi documentali;

CONSIDERATO che una gestione efficiente, trasparente e conforme alla normativa dei flussi documentali è essenziale per l'attività istituzionale e per garantire la tracciabilità delle operazioni;

DETERMINA

1. di adottare il "*Manuale di Gestione*" dei flussi documentali dell'Ordine dei Medici Chirurghi e degli Odontoiatri della Provincia di Campobasso – Versione Ed. 1/2025, che seppur non allegato ne rappresenta parte integrale e sostanziale;
2. di stabilire che il Manuale definisca, tra l'altro:
    a. le responsabilità e i compiti degli attori coinvolti nella produzione, gestione, conservazione e accesso alla documentazione;
    b. i processi operativi standard per protocollazione, registrazione, classificazione, segnatura temporale e archiviazione;
    c. l'uso degli strumenti informatici per l'acquisizione, la firma digitale, l'interscambio e la conservazione digitale a norma;
    d. modalità di accesso ai documenti (interni, esterni, richieste di accesso);
3. di stabilire che la presente Determina e il Manuale adottato vengano pubblicati nel sito istituzionale dell'Ordine.

IL PRESIDENTE
Dr. Giuseppe De Gregorio

GIUSEPPE DE GREGORIO
19.06.2025
09:48:11
GMT+01:00

Manuale di gestione del protocollo informatico, dei flussi documentali e degli archivi dell'Ordine dei Medici Chirurghi e degli Odontoiatri della Provincia di Campobasso

AOO A735DA6

AZIONE	DATA	NOMINATIVO	FUNZIONE
Redazione	16/06/2025	Maria, Giuliana Zicchillo	Funzionario amministrativo
		Edizione 1/2025	
Approvazione		DETERMINA PRESIDENZIALE N. 2 DEL 19/06/2025	

Sommario

Manuale di gestione del protocollo informatico, dei flussi documentali e degli archivi Ordine dei medici chirurghi e degli odontoiatri di Campobasso.....1

1. PRINCIPI GENERALI4

1.1 Premessa 4

Peculiarità dell'Ordine professionale 5

1.2 Ambito di applicazione e struttura del Manuale di Gestione 5

1.2.1 Ambito di applicazione 5

Struttura del manuale 6

1.3 Definizioni e norme di riferimento 6

1.4 Aree organizzative omogenee (AOO) -Unità Organizzative Responsabili (UOR) e modelli organizzativi 7

1.5 Servizio archivistico per la gestione informatica del protocollo informatico, dei flussi documentali e degli archivi 7

1.5.1 Il delegato per la tenuta del protocollo informatico 8

Il delegato per la conservazione 8

Firma digitale (vedi anche cap. 3.4.1) 8

Firma elettronica (vedi anche cap. 3.4.1) 8

Firma remota automatica (vedi anche cap. 3.4.1) 9

1.6 Sistema di protocollo informatico unico e strumenti per il suo funzionamento 9

1.7 Politiche di gestione e conservazione documentale 9

2. PIANO DI SICUREZZA 9

2.1 Formazione dei documenti - aspetti di sicurezza 10

2.2 Gestione dei documenti informatici - aspetti di sicurezza 10

2.2.1 Componente organizzativa della sicurezza 10

Componente fisica e infrastrutturale della sicurezza 10

Componente logica della sicurezza 11

Gestione delle registrazioni di protocollo e di sicurezza 11

Criteri di utilizzo degli strumenti tecnologici 11

2.3 Trasmissione e interscambio dei documenti informatici - aspetti di sicurezza 11

2.4 Accesso ai documenti informatici 11

2.5 Politiche di sicurezza adottate dall'Ente 11

2.6 Servizio archivistico (doc. analogici) 11

3. MODALITÀ DI FORMAZIONE DEI DOCUMENTI 12

3.1 I documenti dell'Ente 12

3.2 Formazione dei documenti 12

Elementi informativi essenziali dei documenti prodotti 12

Formazione dei documenti - aspetti operativi generali 13

3.3 Formazione del documento analogico 13

3.4 Formazione del documento informatico 13

3.5 La firma elettronica (avanzata, qualificata, digitale, automatica) e la validazione temporale..... 143

3.5.1 La Firma Elettronica Remota Automatica Massiva (FERAM) 14

3.6 La validazione temporale 14

3.7 Tipologie di formato del documento informatico 14

3.8 Documenti contenenti collegamenti ipertestuali 144

3.9 Documenti contenenti video o audio o social 15

4. FLUSSI DI LAVORAZIONE DEI DOCUMENTI 15

4.1 Documenti in entrata 15

4.1.2 Ricevuti o prodotti su supporto analogico 15
4.1.3 Ricevuti o prodotti su supporto informatico 15
4.2 Documenti in uscita 15
Inviati su supporto analogico 15
Inviati su supporto informatico 15
4.3 Descrizione del flusso di lavorazione dei documenti 16
5. MODALITÀ DI PRODUZIONE E DI CONSERVAZIONE DELLE REGISTRAZIONI DI PROTOCOLLO INFORMATICO 16
5.1 Registrazione dei documenti 16
5.1.2 Modalità di registrazione di protocollo 16
5.1.3 Documento analogico inviato elettronicamente 17
Documento digitale inviato elettronicamente 17
5.2 Registri di protocollo periodici 17
Invio in conservazione del registro giornaliero di protocollo 17
5.3 La segnatura di protocollo 18
5.4 Procedure specifiche nella registrazione di protocollo 18
5.4.1 Protocollazione di documenti riservati 18
5.4.2 Modifica della gestione della sicurezza per documenti classificati come “riservati” 18
5.4.3 Documenti esclusi dalla registrazione di protocollo 18
5.4.4 Modifica delle registrazioni di protocollo 18
5.4.5 Annullamento delle registrazioni di protocollo 18
5.5 Casi particolari di registrazioni di protocollo 19
5.5.1 Lettere anonime 19
5.5.2 Documenti privi di firma 19
5.5.3 Corrispondenza personale o riservata 19
5.5.4 Integrazioni documentarie 19
5.5.5 Documenti pervenuti per errore all’Ente 19
5.5.6 Trattamento dei documenti con oggetto o smistamento plurimo 19
5.5.7 Documenti in partenza con più destinatari 19
5.5.8 Flussi documentali informatici 19
5.5.8.1 Flusso FNOMCeO-ENPAM 1920
5.5.8.2 Flusso OIL (ordinativo informatico) 20
5.5.8.3 Fatture elettroniche 20
5.5.8.4 Istanze telematiche 20
5.6 Regole di smistamento e di assegnazione 20
5.6.1 Processo di assegnazione dei fascicoli 20
6. MODALITÀ DI UTILIZZO DEL REGISTRO DI EMERGENZA 21
7. SISTEMA DI CLASSIFICAZIONE, FASCICOLAZIONE E PIANO DI CONSERVAZIONE 21
7.1 Protezione e conservazione degli archivi pubblici 21
7.2 Titolario o piano di classificazione 22
7.2.1 Titolario 22
7.2.2 Classificazione dei documenti 22
7.3 Formazione del fascicolo 22
7.3.1 Il fascicolo 22
7.3.2 Famiglie e tipologie di fascicolo 23
7.3.3 Repertorio dei fascicoli 23

7.3.4 Il fascicolo personale dell'iscritto 23
7.3.5 Dossier 24
7.4 Repertori e fascicoli annuali 24
7.5 Tipologie di registri 24
7.6 Organizzazione, gestione e strumenti dell'archivio unico corrente, di deposito e storico 24
7.7 Piano di conservazione 24
7.7.1 Strumenti per la gestione dell'archivio di deposito 25
7.7.2 Obbligo di conservazione, ordinamento e inventariazione dell'archivio storico 25
8. PROCEDIMENTI AMMINISTRATIVI, ACCESSO AI DOCUMENTI E TUTELA DELLA RISERVATEZZA 25
8.1 Premessa 25
8.2 Procedure di accesso ai documenti e di tutela della riservatezza 25
9. APPROVAZIONE E AGGIORNAMENTO DEL MANUALE, NORME TRANSITORIE E FINALI 25
9.1 Modalità di approvazione e aggiornamento del Manuale 25
9.2 Pubblicità del presente Manuale 26
Allegato 1 - Glossario dei termini e degli acronimi 277
Allegato 2 - Individuazione AOO 30
Allegato 3 – Organigramma 3030
Allegato 4 - Istituzione servizio archivistico e nomina del responsabile 3030
Allegato 5 – Titolario (proposto dal gruppo sulla gestione documentale della FNOMCeO ed approvato dalla sovraintendenza del Lazio) 3031
Allegato 6 – Oggettario 355
Allegato 7 – Piano di fascicolazione 444
Allegati 8 A e 8 B – Regolamento Privacy OMCeO di Campobasso e Registro delle attività di trattamento dati 555
Allegato 9 - Art. 54-bis del Decreto legislativo 30 marzo 2001, n. 165 e art. 3 della Legge n 179 del 2017 566
Allegato 10 – Registro degli eventi di violazione dei dati personali e modello segnalazione data breach 566
Allegato 11 - Formati di file e riversamento dell'ente 6262
Allegato 12 – Documenti esclusi dal protocollo 6464
Allegato 13 – Registro di protocollo di emergenza 65

1. PRINCIPI GENERALI

1.1 Premessa

Il Decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013 concernente le "*Regole tecniche per il protocollo informatico*" ai sensi del Codice dell'Amministrazione Digitale di cui al decreto legislativo n. 82 del 2005, all'art. 3, comma 1, lettera d), prevede per tutte le amministrazioni di cui all'art. 2, comma 2, l'adozione del Manuale di gestione.

Il Manuale di gestione, disciplinato dal successivo art. 5, comma 1, "descrive il sistema di gestione, anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi".

In questo ambito è previsto che ogni Amministrazione Pubblica individui una o più Aree Organizzative Omogenee, all'interno delle quali sia nominato un Responsabile del Servizio per la tenuta del protocollo informatico, così come già previsto dall'art. 50, comma 4 del Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa - Decreto del Presidente della Repubblica n. 445 del 20 dicembre 2000.

Obiettivo del manuale di gestione è descrivere il sistema di gestione documentale a partire dalla fase di registrazione dei documenti; elencare le ulteriori funzionalità disponibili nel sistema, finalizzate alla gestione di particolari tipi di documenti, alla pubblicità legale degli atti e documenti nelle modalità previste dalla normativa vigente e alla acquisizione e gestione di documenti redatti mediante i moduli e formulari disponibili sul portale istituzionale dell'Ordine.

Il presente manuale è frutto di un lavoro congiunto di un Gruppo di Lavoro di Funzionari appartenenti a diversi Ordini Provinciali dei Medici Chirurghi e degli Odontoiatri, col supporto della Prof.ssa Guercio di ANAI ed è un documento work in progress, al fine di migliorarlo ed adeguarlo alle nuove indicazioni di AGID.

Il documento Manuale di gestione dovrà, quindi, essere periodicamente aggiornato sulla base delle evoluzioni organizzative, normative, tecnologiche e degli strumenti informatici utilizzati.

Il protocollo informatico, anche con le sue funzionalità minime, costituisce l'infrastruttura di base tecnico-funzionale sulla quale avviare il processo di ammodernamento e di trasparenza dell'attività dell'amministrazione.

Il presente documento, pertanto, si rivolge non solo agli operatori del sistema di gestione documentale e di protocollo, ma, in generale, a tutti i dipendenti e ai soggetti esterni che si relazionano con l'amministrazione.

Il protocollo informatico e il sistema di gestione documentale costituiscono il fulcro della struttura tecnologica e organizzativa dell'Ente con riferimento alla gestione dei documenti, dei flussi documentali, dei processi e dei procedimenti amministrativi, nel rispetto della normativa vigente.

Il registro di protocollo è atto di fede privilegiata[1] perché prodotto durante l'espletamento dell'attività di un pubblico ufficiale e questo lo qualifica come atto pubblico che non necessita, tra i requisiti essenziali per la sua efficacia, di una sottoscrizione (firma).

I fattori che garantiscono il valore probatorio del registro di protocollo informatico sono:

- l'appartenenza del fatto attestato alla sfera di attività direttamente compiuta dal pubblico ufficiale;
- il dirigente o funzionario che presiede alla sua compilazione attestandone il contenuto;
- il requisito di immodificabilità imposto nelle operazioni di registrazione e il tracciamento delle azioni di annullamento o correzione;
- i requisiti di sicurezza del sistema.

Peculiarità dell'Ordine professionale

L'Ordine dei Medici Chirurghi e degli Odontoiatri della Provincia di Campobasso, di seguito "Ente", è un ente pubblico non economico sussidiario dello Stato dotato di una struttura organizzativa semplice e poco ramificata.

Inoltre, la limitata numerosità del personale e la relativa concentrazione delle funzioni/attività, riduce notevolmente le esigenze gestionali.

Gli iter amministrativi avvengono quasi sempre all'interno dello stesso ufficio e i documenti vengono presi in carico spesso dagli stessi addetti che effettuano le registrazioni di protocollo.

Ciò premesso l'Ente intende adempiere agli obblighi normativi applicando le prescrizioni, in un'ottica di semplificazione dei processi, degli strumenti e riduzione dei costi.

L'organizzazione degli uffici, in considerazione della tipologia e della funzione svolta, presentano esigenze di semplificazione della gestione documentale, che pertanto viene svolta in maniera coordinata e unitaria da un'unica AREA ORGANIZZATIVA OMOGENEA (AOO).

1.2 Ambito di applicazione e struttura del Manuale di Gestione

1.2.1 Ambito di applicazione

Il Manuale è destinato alla più ampia diffusione interna ed esterna, in quanto fornisce le istruzioni complete per la corretta gestione dei documenti, che comprende le attività di:

- formazione
- gestione
- registrazione
- classificazione
- fascicolazione
- archiviazione
- conservazione

dei documenti.

Come prescritto **dall'art. 5, comma 3 del DPCM 13 novembre 2013 Regole tecniche per il protocollo informatico**, è pubblicato sul sito istituzionale dell'Ente.

Esso disciplina:

- il piano di sicurezza dei documenti
- le modalità di formazione e scambio dei documenti
- l'utilizzo del sistema di protocollo informatico e gestione documentale
- la gestione dei flussi documentali, sia cartacei che digitali e le aggregazioni documentali (fascicoli)
- l'uso del Titolario di classificazione e del piano di conservazione
- le modalità di accesso ai documenti e alle informazioni e le relative responsabilità
- la gestione dei procedimenti amministrativi

[1] Il Consiglio di Stato (Sent. 1993, I, 838) ha riconosciuto il protocollo come atto pubblico di "fede privilegiata". Nella gerarchia dei mezzi probatori documentali, al documento regolarmente protocollato è assegnato un rango superiore rispetto agli altri mezzi di prova, in quanto si presenta come atto pubblico gerarchicamente più elevato.

Il presente Manuale di gestione è adottato dall'Ente ai sensi dell'art. 3, comma 1, lettera d) del decreto del Presidente del Consiglio dei ministri 3 dicembre 2013, recante le regole tecniche per il protocollo informatico.

L'adozione del Manuale di gestione si pone l'obiettivo di raggiungere, attraverso i sistemi che l'Ente ha a disposizione per la gestione documentale, una corretta ed uniforme metodologia per il trattamento dei documenti sia analogici che digitali, una serie di procedure condivise per la gestione dei procedimenti amministrativi, l'accesso agli atti ed alle informazioni e l'archiviazione e la conservazione dei documenti.

Struttura del Manuale

L'attuale Manuale di gestione è organizzato in 9 capitoli ed include n. 13 allegati.

1.3 Definizioni e norme di riferimento

Ai fini delle definizioni del presente Manuale si è fatto riferimento alla seguente normativa e documentazione:

RD 1163/1911, *Regolamento per gli archivi di Stato*;

DPR 1409/1963, *Norme relative all'ordinamento ed al personale degli archivi di Stato*;

Legge 241/1990, *Nuove norme sul procedimento amministrativo;*

DPR 445/2000, *Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;*

DPR 37/2001, *Regolamento di semplificazione dei procedimenti di costituzione e rinnovo delle Commissioni di sorveglianza sugli archivi e per lo scarto dei documenti degli uffici dello Stato;*

D.lgs 196/2003 recante il *Codice in materia di protezione dei dati personali;*

D.lgs 42/2004, *Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137;*

Legge 9 gennaio 2004, n. 4 aggiornata dal decreto legislativo 10 agosto 2018, n. 106, *Disposizioni per favorire e semplificare l'accesso degli utenti e, in particolare, delle persone con disabilità agli strumenti informatici;*

D.lgs 82/2005 e ss.mm.ii., *Codice dell'amministrazione digitale;*

D.lgs 33/2013, *Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni;*

DPCM 22 febbraio 2013, *Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71;*

DPCM 21 marzo 2013, *Individuazione di particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico, ai sensi dell'art. 22, comma 5, del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni;*

Reg. UE 910/2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE - *Regolamento eIDAS;*

Circolare 40 e 41 del 14 dicembre 2015 della Direzione generale degli archivi, Autorizzazione alla distruzione di originali analogici riprodotti secondo le regole tecniche di cui al DPCM 13.11.2014 e conservati secondo le regole tecniche di cui al DPCM 13.12.2013;

Reg. UE 679/2016 (GDPR), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;

Circolare 18 aprile 2017, n. 2/2017 dell'Agenzia per l'Italia Digitale, recante le misure minime di sicurezza ICT per le pubbliche amministrazioni;

Circolare n. 2 del 9 aprile 2018, recante i criteri per la qualificazione dei Cloud Service Provider per la PA;

Circolare n. 3 del 9 aprile 2018, recante i criteri per la qualificazione di servizi SaaS per il Cloud della PA;

Reg. UE 2018/1807, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea;

DPCM 19 giugno 2019, n. 76, *Regolamento di organizzazione del Ministero per i beni e le attività culturali, degli uffici di diretta collaborazione del Ministro e dell'Organismo indipendente di valutazione della performance.*

Linee guida AgID richiamate

Linee guida del 15 aprile 2019 dell'indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi;

Linee guida del 6 giugno 2019 contenenti le Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate.

Linee guida del 09/01/2020 sull'Accessibilità degli strumenti informatici.

Linee guida del Maggio 2021 sulla formazione, gestione e conservazione dei documenti informatici.

Ai fini del presente manuale si intende per:

"**Ente**", l'Ordine dei Medici Chirurghi e degli Odontoiatri della Provincia di Campobasso;

"**Testo Unico**", il decreto del Presidente della Repubblica 20 dicembre 2000, n. 445 – *"Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa";*

"**Regole tecniche**", il decreto del Presidente del Consiglio dei ministri 3 dicembre 2013 concernente le *"Regole tecniche per il protocollo informatico"*

"**Codice**" o **"CAD",** il decreto legislativo 7 marzo 2005, n. 82 - *Codice dell'Amministrazione Digitale e successive modificazioni* (ultimo aggiornamento all'atto pubblicato il 29/01/2025 (GU n.112 del 16-05-2005 - Suppl. Ordinario n. 93).

Di seguito si riportano gli acronimi utilizzati più frequentemente:

AOO - Area Organizzativa Omogenea

DPO – Data Protection Officer

MdG - Manuale di Gestione del protocollo informatico, gestione documentale e degli archivi (il presente documento)

RPA - Responsabile del Procedimento Amministrativo - il dipendente che ha la responsabilità dell'esecuzione degli adempimenti amministrativi relativi ad un affare

RSI - Responsabile della Sicurezza Informatica

RSP - Responsabile del Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi

SGD – Servizio gestione documentale

UOR - Uffici Organizzativi di Riferimento - un insieme di uffici che, per tipologia di mandato istituzionale e competenza, di funzione amministrativa perseguita, di obiettivi e di attività svolta, presentano esigenze di gestione della documentazione in modo unitario e coordinato

Per altre definizioni si faccia riferimento all'*Allegato 1 - Glossario dei termini e degli acronimi*

1.4 Aree organizzative omogenee (AOO) -Unità Organizzative Responsabili (UOR) e modelli organizzativi

Ai fini della gestione unica e coordinata dei documenti l'Ente è costituito da un'unica Area organizzativa omogenea (AOO unica) - ***si veda Allegato 2 - Individuazione Area organizzativa omogenea (AOO unica)***.

All'interno della AOO viene utilizzato un unico sistema di protocollazione che consente l'autonomia di ogni UOR per la registrazione della corrispondenza in entrata, in uscita ed interna.

Le Unità organizzative responsabili (UOR) sono individuate dall'organigramma dell'Ente **(si veda *Allegato 3 - Organigramma*)**.

1.5 Servizio archivistico per la gestione informatica del protocollo informatico, dei flussi documentali e degli archivi

A norma dell'art. 61 del DPR 445/2000, Il Consiglio Direttivo ha istituito, con Deliberazione n. 64 del 09/06/2025, l'ufficio denominato "Servizio archivistico dell'Ordine dei Medici chirurghi e degli Odontoiatri di Campobasso", con il compito di gestire il protocollo informatico, i flussi documentali e gli archivi.

Al Servizio archivistico è demandata la gestione dell'archivio (corrente, di deposito e storico), che comprende:

la gestione e il coordinamento del sistema di protocollo informatico: registrazione, classificazione, assegnazione dei documenti, costituzione e repertoriazione dei fascicoli, autorizzazione per l'accesso alle funzioni della procedura, gestione del registro di emergenza, annullamento di registrazioni;
la gestione e il coordinamento degli archivi:

- **corrente:** riguarda i documenti necessari alle attività correnti;
- **di deposito:** riguarda i documenti ancora utili per finalità amministrative o giuridiche, ma non più indispensabili per la trattazione delle attività correnti;
- **storico:** riguarda i documenti storici selezionati per la conservazione permanente.

Con la medesima Deliberazione si individua il Responsabile del Servizio per la tenuta del protocollo informatico che, a norma dell'art. 61, comma 2 del DPR 445/2000, è definito come un "**dirigente, ovvero un funzionario, in possesso di idonei requisiti professionali o di professionalità tecnico archivistica acquisita a seguito di processi di formazione definiti secondo le procedure prescritte dalla disciplina vigente**".

In mancanza di una figura dirigenziale, si individua il dipendente che, in possesso di idonei requisiti di cui sopra, sia nelle condizioni di poter assolvere all'incarico.

La gestione dell'Ufficio è affidata pertanto al Funzionario (qualifica funzionale risultante in Pianta Organica) DOTT.SSA MARIA, GIULIANA ZICCHILLO ***(si veda Allegato 4 - Istituzione del Servizio archivistico dell'Ordine dei medici chirurghi e degli odontoiatri e individuazione del responsabile).***

In assenza del responsabile le decisioni vengono assunte da un suo delegato o alternativamente dal Segretario dell'Ente ovvero dal Presidente e legale rappresentante.

Ai sensi dell'art. 4, comma 1 del DPCM 13 novembre 2013 *Regole tecniche per il protocollo informatico* sono compiti del Responsabile del Servizio:

- predisporre lo schema del Manuale di gestione di cui all'art. 5 delle "Regole tecniche per il protocollo";
- curare la redazione e l'aggiornamento del Titolario, del Piano di fascicolazione e degli altri strumenti archivistici previsti;

- proporre i tempi, le modalità e le misure organizzative e tecniche finalizzate alla eliminazione dei protocolli di settore e di reparto, dei protocolli multipli e, più in generale, dei protocolli diversi dal protocollo informatico;
- predisporre il piano per la sicurezza informatica relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici nel rispetto delle misure minime di sicurezza previste nel disciplinare tecnico pubblicato in allegato B del decreto legislativo 30 giugno 2003, n. 196 e successive modificazioni e dalla circolare AgID del 18 aprile 2017 n. 2/201 che definisce le misure di sicurezza, d'intesa con il responsabile della conservazione, con i preposti ai sistemi informativi (Amministratore di sistema) e con il responsabile del trattamento dei dati personali di cui al suddetto decreto.

Sono inoltre compiti del Servizio:

- abilitare gli addetti dell'amministrazione all'utilizzo del sistema di protocollo informatico e definire per ciascuno di essi il tipo di funzioni disponibili (ad esempio consultazione, registrazione, modifica ecc.);
- garantire il rispetto delle disposizioni normative durante le operazioni di registrazione e di segnatura di protocollo garantire la corretta produzione e conservazione del registro giornaliero di protocollo;
- curare le funzionalità del sistema affinché, in caso di guasti o anomalie, siano ripristinate entro ventiquattro ore dal blocco delle attività e, comunque, nel più breve tempo possibile;
- conservare le copie di salvataggio delle informazioni del sistema di protocollo e del registro di emergenza in luoghi sicuri e diversi da quello in cui viene custodito il suddetto sistema;
- garantire il buon funzionamento degli strumenti e il rispetto delle procedure concernenti le attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali autorizzare le operazioni di annullamento delle registrazioni di protocollo;
- aprire e chiudere il registro di emergenza;
- definire e assicurare criteri uniformi di trattamento del documento informatico e, in particolare, di classificazione ed archiviazione, nonché di comunicazione interna, ai sensi dell'art. 50, comma 4, del Testo Unico;
- autorizzare, aprire, chiudere e assicurarsi della corretta compilazione dell'eventuale protocollo di emergenza.

1.5.1 Il delegato per la tenuta del protocollo informatico

È in facoltà del Responsabile avvalersi della delega di funzioni a dipendenti dell'Ente in possesso dei necessari requisiti di competenza e professionalità.

I compiti del delegato per la tenuta del protocollo informatico sono:

- garantire il rispetto delle disposizioni normative e delle procedure durante le operazioni di registrazione e di segnatura di protocollo;
- autorizzare le operazioni di annullamento della registrazione di protocollo;
- garantire la corretta produzione e conservazione del registro giornaliero di protocollo;
- conservare le copie di salvataggio del registro giornaliero di protocollo e del registro di emergenza in sistemi diversi da quello in cui opera il sistema di gestione del protocollo;
- aprire e chiudere il registro di protocollazione di emergenza.

Il delegato si avvale di sostituti in caso di sua assenza o impedimento.

Quando non vi sia la nomina del delegato, tali funzioni sono assunte dal responsabile del servizio archivistico e protocollo informatico.

Il delegato per la conservazione

Il servizio di conservazione digitale dei documenti è affidato a fornitore esterno.

Il delegato interno per la conservazione svolge i seguenti compiti:

- affianca il RUP nella verifica dei requisiti di legge nella scelta del fornitore di conservazione;
- verifica il manuale della conservazione redatto dal fornitore da integrare con il manuale di conservazione dell'organizzazione;
- interagisce con il fornitore per la definizione dei metadati da utilizzare per ogni tipologia documentale da portare in conservazione;
- definisce contrattualmente i tempi di conservazione dei documenti;
- effettua verifiche periodiche di mantenimento dei requisiti del fornitore (esempio controlli a campione sui documenti e richieste di pacchetti di distribuzione).

Il delegato si avvale di sostituti in caso di sua assenza o impedimento.

Quando non vi sia la nomina del delegato, tali funzioni sono assunte dal responsabile del servizio archivistico e protocollo informatico

Firma digitale (vedi anche cap. 3.4.1)

L'Ente utilizza la firma digitale per l'espletamento delle attività istituzionali e gestionali con la finalità, ai sensi del CAD, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.

Tutti i dipendenti dell'Ente, che ne avessero necessità per motivi di servizio, sono muniti di firma digitale.

Nella gestione delle firme digitali si tiene conto che il loro rinnovo (ogni 3 anni) deve avvenire prima della loro scadenza. Al fine di minimizzare la possibilità di superare tale limite temporale, le procedure di rinnovo vengono avviate almeno 30 gg prima della scadenza di ogni certificato di firma.

Firma elettronica (vedi anche cap. 3.4.1)

In conformità alla normativa vigente in materia di amministrazione digitale, le credenziali di accesso costituiscono la "firma elettronica" dell'utente che utilizza il sistema e qualsiasi azione e attività svolta nel sistema documentale e del protocollo, costituisce atto valido ai fini amministrativi. Si sottolinea l'importanza della segretezza delle credenziali e del cambio password periodico, in base alle politiche di sicurezza dell'Ente (si raccomanda il cambio password ogni 3 mesi).

Firma remota automatica (vedi anche cap. 3.4.1)

Il responsabile del protocollo è dotato di firma automatica per l'espletamento delle procedure di firma massiva connesse al sistema di riversamento in conservazione del registro giornaliero di protocollo, per procedura di attestazione di conformità o per procedure di firma singola o multipla di documenti generati automaticamente.

1.6 Sistema di protocollo informatico unico e strumenti per il suo funzionamento

L'Ente, avendo individuato un'unica AOO, dispone di un unico sistema di protocollo informatico e gestione documentale denominato "*IrideDoc - Protocollo Informatico, Gestione Documentale e Conservazione Digitale*" (di seguito software di protocollo) prodotto da TECSIS S.r.l., Viale Svezia 16 - 35020 -Ponte San Nicolò - Padova – Italy, P. IVA/C.F. 03719260287, Registro Imprese di Padova n. 03719260287, Numero R.E.A 331324.

IrideDoc è il software per la tenuta del protocollo informatico e l'archiviazione documentale che garantisce il rispetto di standard di sicurezza, autenticità, integrità, riservatezza e conservazione a lungo termine. Si tratta di un sistema integrato che permette agli enti pubblici e organizzazioni di registrare, archiviare e consultare documenti in modo digitale, minimizzando il ricorso alla documentazione cartacea e favorendo la digitalizzazione e la trasparenza.

Il software è conforme a quanto richiesto dal DPR 445/2000, dalle regole tecniche derivate dal CAD e sempre in aggiornamento per essere allineato alle ultime Linee Guida AGID.

Con *IrideDoc* si può svolgere una gestione documentale improntata sui principi archivistici permettendo così una gestione avanzata dei flussi documentali.

Il software è predisposto per l'archiviazione a norma e conservazione digitale con l'utilizzo di conservatori esterni qualificati, uno privato, Namirial, ed uno pubblico, Il PARER (Polo Archivistico Regionale dell'Emilia Romagna).

IrideDoc ha anche la gestione integrata, *Irideweb*, che permette la protocollazione automatica di tutte le istanze inviate dai professionisti e tutta la documentazione prodotta dall'Ente da *IrideOnline*.

Il software permette di:

- generare protocolli in entrata e uscita;
- gestire l'annullamento di un protocollo con possibilità di duplicazione del protocollo annullato;
- gestire le registrazioni interne;
- gestire soggetti con sincronizzazione dei dati da Iride Online;
- gestire i registri di emergenza;
- gestire le aggregazioni documentarie (fascicoli, repertori, dossier);
- scaricare la posta da mail e/o PEC;
- inviare documenti protocollati tramite mail e/o PEC;
- generare, firmare, protocollare ed inviare in conservazione il registro giornaliero di protocollo;
- gestire documenti con firma digitale integrata per l'attestazione di conformità;
- connessione con SdI per protocollazione automatica delle fatture elettroniche;
- connettore con Iride Online per protocollazione automatica di tutta la documentazione generata dal software dell'anagrafica;
- gestione assegnazioni di protocolli e/o fascicoli.

Il protocollo informatico unico è lo strumento attraverso il quale l'Ente garantisce l'effettiva ricezione e trasmissione dei documenti. Con la messa a regime di tale sistema è cessata di fatto la necessità di mantenere altri protocolli interni (protocolli di settore, servizio, ufficio, etc., protocolli multipli, etc.) o altri sistemi di registrazione diversi dal protocollo unico, che sono stati eliminati.

Al protocollo informatico unico sono di supporto i seguenti strumenti di gestione se presenti:

Titolario di classificazione (***Allegato 5 - Titolario di classificazione***)
Oggettario (***Allegato 6 – Oggettario documento in continua evoluzione ed ampliamento***)
Organigramma (***Allegato 3 - Organigramma***)
Repertorio dei fascicoli (da produrre a fine anno)
Piano di fascicolazione ***(Allegato 7 - Piano di fascicolazione)***
Piano di conservazione e scarto (in fase di definizione)
Elenco dei formati di file e riversamento (***Allegato 11 - Formati di file e riversamento dell'Ente***)

1.7 Politiche di gestione e conservazione documentale

L'Ente ha adottato e programmerà nel futuro politiche di gestione e conservazione in linea con la normativa vigente e, con riferimento specifico al Manuale di gestione qui proposto, coerenti con il Codice dei beni culturali e con il Codice dell'amministrazione digitale (CAD).

La gestione e la conservazione hanno come obiettivo la tutela dei documenti nel loro valore giuridico-probatorio mantenendo l'integrità e affidabilità, e la valorizzazione finalizzata alla fruibilità a scopi storici delle informazioni e dei dati contenuti nei documenti.

L'Ente si avvale di un conservatore esterno scelto dall'elenco dei conservatori attivi qualificati presso AgID, secondo i criteri e le modalità descritte nella Linee guida AgID maggio 2021. Il Software di gestione del protocollo e dei documenti consente il riversamento con modalità semplificate.

2. PIANO DI SICUREZZA

Il presente capitolo, ai sensi **delle misure minime di sicurezza ICT emanate dall'AgID con circolare del 18 aprile 2017, n. 2/2017 e ai sensi dell'art. 32 del Regolamento UE 679/2016 (GDPR)**, riporta le misure di sicurezza adottate per la formazione, la gestione, la trasmissione, l'interscambio, l'accesso e la conservazione dei documenti informatici, nel rispetto delle misure minime di sicurezza.

2.1 Formazione dei documenti - aspetti di sicurezza

Le risorse strumentali e le procedure atte a garantire la sicurezza nella formazione dei documenti informatici, con particolare riferimento alla loro immodificabilità e integrità, sono descritte nel cap.3.

2.2 Gestione dei documenti informatici - aspetti di sicurezza

Il sistema di gestione informatica dei documenti:

- garantisce la disponibilità, la riservatezza e l'integrità dei documenti e del registro di protocollo;
- assicura la corretta e puntuale registrazione di protocollo dei documenti in entrata ed in uscita;
- fornisce informazioni sul collegamento esistente tra ciascun documento ricevuto dall'Ente e gli atti dalla stessa formati al fine dell'adozione del provvedimento finale;
- consente il reperimento delle informazioni riguardanti i documenti registrati;
- permette, in condizioni di sicurezza, l'accesso alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di "privacy" con particolare riferimento al trattamento dei dati sensibili e giudiziari;
- garantisce la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato.

2.2.1 Componente organizzativa della sicurezza

Tale componente consiste nella definizione di una struttura operativa dedicata alla gestione della sicurezza nell'ambito delle attività svolte per il protocollo e gestione documentale.

In tale contesto la gestione della sicurezza si realizza con specifici interventi tecnici e organizzativi finalizzati a prevenire, contrastare o ridurre gli effetti relativi ad una specifica minaccia e con attività di controllo e verifica essenziali ad assicurare l'efficacia nel tempo del sistema informatico.

Conseguentemente vengono adottate le seguenti misure di sicurezza, la cui competenza è posta a carico di figure che sono appositamente individuate come previsto dalla normativa vigente.

Le nomine nell'ambito della sicurezza sono indicate nell'***Allegato 8 A**: Regolamento per la tutela delle persone fisiche con riguardo al trattamento dei dati personali* *(Deliberazione CD n. 32 del 12/01/2022)* e nell'***Allegato 8 B: Registro delle Attività di Trattamento (Responsabile del Trattamento).***

Componente fisica e infrastrutturale della sicurezza

La sede è organizzata in due diverse aree:

- area di accesso al pubblico
- area di lavoro riservata

II controllo degli accessi fisici alle risorse dell'area di lavoro riservata, è regolato secondo i seguenti principi:

- l'accesso è controllato e consentito soltanto al personale autorizzato per motivi di servizio;
- i meccanismi di controllo dell'accesso sono più selettivi all'aumentare della sensibilità dei dati custoditi e quindi del livello di protezione del locale necessario;
- gli utenti dei servizi dell'Ente, i visitatori occasionali, i dipendenti di aziende esterne e gli ospiti, possono accedere esclusivamente alle aree pubbliche. Gli accessi alle aree protette possono avvenire solo a seguito di procedura di identificazione. Essi non possono entrare e trattenersi nelle aree protette se non accompagnati da personale dell'Ente autorizzato a quel livello di protezione;
- gli addetti dell'impresa di pulizie hanno accesso alle aree protette durante l''orario di ufficio;
- ogni persona che accede alle risorse della sede in locali protetti è identificata in modo certo.

Le misure di sicurezza fisica hanno un'architettura multilivello così articolata:

- a livello di edificio, attengono alla sicurezza perimetrale e sono atte a controllare l'accesso alla sede in cui sono ospitate risorse umane e strumentali;
- a livello di locale, sono finalizzate a controllare l'accesso ai locali interni alla sede.

Il controllo degli accessi fisici alle risorse della sede dell'Ente/AOO è regolato secondo i principi stabiliti dell'Ente.

Si garantisce la sicurezza fisica degli accessi fisici ai luoghi in cui sono custodite le risorse del sistema informatico attraverso locali dotati di:

- porta blindata all'ingresso principale;
- armadi dotati di serrature;
- impianti elettrici verificati;
- luci di emergenza;
- sistemi di condizionamento per il raffreddamento delle apparecchiature;
- continuità elettrica del server garantita da apposito UPS;
- continuità elettrica per i soli computer client degli uffici operativi;
- estintori;
- controllo dell'attuazione del piano di verifica periodica dell'efficacia degli estintori.

Essendo la Sede operativa lontana da insediamenti industriali e posta all'interno di un edificio adibito ad abitazioni private e uffici, le sue condizioni ambientali per quanto riguarda polvere, temperatura, umidità, vibrazioni meccaniche, interferenze elettriche e radiazioni elettromagnetiche e livelli

di inquinamento chimico e biologico, sono tali da non richiedere misure specifiche di prevenzione oltre quelle già adottate per le sedi di uffici di civile impiego.

Componente logica della sicurezza e gestione delle registrazioni di protocollo e di sicurezza

La componente logica della sicurezza e la gestione delle registrazioni di protocollo e di sicurezza garantiscono i requisiti di integrità, riservatezza, disponibilità e non ripudio dei dati, delle informazioni e dei messaggi.

Tale componente, nell'ambito del sistema di protocollo informatico e di gestione documentale, è stata realizzata attraverso:

- identificazione e autenticazione utente;
- profilazione degli accessi (ACL - Access Control List);
- sistemi antivirus;
- firma digitale (dove necessario);
- monitoraggio sessioni di lavoro;
- disponibilità del software e dell'hardware;
- ridondanza dei sistemi di salvataggio;
- replica del salvataggio in Cloud (in area geografica diversa da quella dell'Ente ma comunque in Paese della UE).

Le realizzazioni sono in parte in carico al software specifico e in parte all'infrastruttura in cui il software è stato installato e viene utilizzato.

Criteri di utilizzo degli strumenti tecnologici

Il sistema informatico garantisce agli utenti interni dell'Ente l'accesso ai servizi previsti mediante l'adozione di un insieme di misure organizzative e tecnologiche.

Gli utenti interni autorizzati ad utilizzare il software di protocollo, operano nel rispetto del "Codice di comportamento dei dipendenti pubblici" emanato con D.P.R. 62/2013 e modificato con D.P.R. 81/2023, cui si richiama integralmente *(**Allegato n. 9: art. 54 comma 1-bis, Decreto Legislativo 30 marzo 2001, N. 165).***

2.3 Trasmissione e interscambio dei documenti informatici - aspetti di sicurezza

L'Ente predilige l'utilizzo di tecnologie di trasmissione sicure.

Si veda l'Art. 51 "Sicurezza dei dati" del Codice di Amministrazione Digitale vigente.

2.4 Accesso ai documenti informatici

Il controllo degli accessi è assicurato utilizzando le credenziali di accesso (pubblica e privata o PIN nel caso di un dispositivo rimovibile in uso esclusivo all'utente) ed un sistema di autorizzazione basato sulla profilazione degli utenti in via preventiva.

2.5 Politiche di sicurezza adottate dall'Ente

Le politiche di sicurezza stabiliscono sia le misure preventive per la tutela e l'accesso al patrimonio informativo, sia le misure per la gestione degli incidenti informatici.

Come previsto dal provvedimento 393, 2 luglio 2015 del Garante della protezione dei dati personali, le amministrazioni pubbliche sono tenute a comunicare al Garante le violazioni dei dati personali (data breach) che si verificano nell'ambito delle banche dati (qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti, art. 4, comma 1, lett. p del Codice in materia di protezione dei dati personali 196 del 2003) di cui sono titolari, secondo la compilazione del modulo predisposto dal Garante (***Allegato 10: Registro degli eventi di violazione dei dati personali e modello segnalazione data breach***)

La figura professionale responsabile della sicurezza informatica nella Pubblica Amministrazione è quella del Responsabile della Sicurezza Informatica (RSI), anche noto come Chief Information Security Officer (CISO). Si tratta di un ruolo oggi fondamentale per garantire che tutte le risorse tecnologiche e i sistemi informativi della PA siano protetti da minacce informatiche e che vengano rispettate le normative nazionali e internazionali sulla protezione dei dati.

Il RSI ha la responsabilità di sviluppare, implementare e gestire le politiche di sicurezza informatica, in linea con la normativa vigente, come il Regolamento europeo 2016/679 (GDPR) e le leggi italiane in materia di protezione dei dati. Inoltre deve assicurarsi che i sistemi informatici e le infrastrutture tecnologiche siano protetti da cyberattacchi, come malware, ransomware e phishing, per esempio con l'utilizzo di software adeguati come quelli sviluppati da Impresoft per il settore pubblico.

Per l'OMCeO di Campobasso, l'individuazione di tale figura è ad oggi in via di definizione. Sarà compito del Responsabile della sicurezza del sistema informatico e del Responsabile della tutela dei dati personali, procedere al perfezionamento, alla divulgazione, al riesame e alla verifica delle politiche di sicurezza.

Il riesame delle politiche di sicurezza è conseguente al verificarsi di incidenti di sicurezza, di variazioni tecnologiche significative, di modifiche all'architettura di sicurezza che potrebbero incidere sulla capacità di mantenere gli obiettivi di sicurezza o portare alla modifica del livello di sicurezza complessivo, ad aggiornamenti delle prescrizioni minime di sicurezza richieste dall'Agenzia per l'Italia digitale o a seguito dei risultati delle attività di audit.

2.6 Servizio archivistico (doc. analogici)

La sede dell'archivio dell'Ente è individuata in Via Mazzini, 129/A, 86100 Campobasso.
I dati in formato digitale sono memorizzati all'interno delle postazioni di lavoro assegnate agli uffici e nel server dell'Ente.

I dati in formato cartaceo sono custoditi in armadi dotati di serratura e conservati per il tempo necessario al conseguimento delle finalità per le quali sono stati raccolti o per un periodo ulteriore se così disposto dalle norme di diritto, nonché dalle normative in materia di tenuta della documentazione amministrativa o qualora si renda necessario proseguire nell'archiviazione ai fini del pubblico interesse.
Per il requisito di "accesso e consultazione", l'AOO garantisce la leggibilità, nel tempo, di tutti i documenti trasmessi o ricevuti, adottando i formati previsti dalle regole tecniche vigenti.
L'accesso agli atti ovvero ai documenti contenuti nell'archivio è disciplinato dall'Art. 24 della Legge 241/1990 e s.m.i., dal suo Regolamento attuativo e dal Regolamento dell'Ordine relativo all'accesso degli atti amministrativi pubblicato sul sito istituzionale dell'Ente al seguente link: https://www.ordinedeimedici.cb.it/wp-content/uploads/2018/07/Regolamento-per-l%E2%80%99esercizio-del-diritto-di-Accesso-ai-documenti-amministrativi-.pdf

La domanda di accesso ai documenti viene presentata all'Ufficio di Segreteria. Ricevuta la richiesta di accesso agli atti, l'Ente provvede ad avviare il procedimento conformemente alla normativa sopra citata.
La consultazione dei documenti è possibile esclusivamente sotto la diretta sorveglianza del personale addetto.
In caso di pratiche momentaneamente irreperibili, in cattivo stato di conservazione, in restauro o in rilegatura, il Responsabile della gestione documentale rilascia apposita dichiarazione entro il termine di 30 giorni. In caso di pratiche escluse dal diritto di accesso conformemente alla normativa vigente, il responsabile del procedimento competente per la pratica oggetto di accesso rilascia apposita dichiarazione entro il termine di 30 giorni.
L'accesso al materiale dell'archivio è consentito dal responsabile del procedimento competente per la pratica oggetto di accesso.
Gli Uffici di Segreteria, per motivi di consultazione, possono richiedere in ogni momento al servizio archivistico i fascicoli conservati presso la sede dell'Ordine.
Il Responsabile della gestione documentale verifica che la restituzione dei fascicoli affidati temporaneamente avvenga alla scadenza prevista. L'affidatario dei documenti non estrae i documenti originali dal fascicolo, né altera l'ordine, rispettandone la sedimentazione archivistica e il loro vincolo.
È presente presso la sede anche una cassaforte dotata di combinazione e chiave contenente vario materiale contabile, una piccola somma di cassa in contanti ed alcuni valori preziosi. Solo il Presidente/Rappresentante legale è autorizzato ad aprirla.
I soggetti esterni che accedono ai locali dell'Ente per le varie manutenzioni hanno accesso senza particolari formalità, previo riconoscimento e sotto la sorveglianza del personale di segreteria.
Il personale della ditta delle pulizie accede ai locali sotto la stretta responsabilità del legale rappresentante della ditta che ha ottenuto il contratto per il servizio a seguito di affidamento pubblico. Egli è direttamente responsabile del proprio personale e ne regola l'accesso in sicurezza ai locali.
Il Codice di comportamento del personale dipendente dell'Ordine si applica anche a tutti i soggetti esterni all'Ente che svolgono le proprie attività presso l'Ente, che pertanto dovranno garantire in ogni momento anche la sicurezza degli archivi dell'ente ed avere un comportamento consono i doveri minimi di lealtà, correttezza e riservatezza.

3. MODALITÀ DI FORMAZIONE DEI DOCUMENTI

3.1 I documenti dell'Ente

I documenti dell'Ente (d'ora in poi chiamati semplicemente documenti) sono quelli prodotti (spediti e ricevuti), in uno dei modi previsti dal CAD in vigore, dagli organi e uffici dell'Ente medesimo nello svolgimento dell'attività istituzionale.

In ottemperanza a quanto indicato dal vigente Codice dell'amministrazione digitale, che prevede l'uso delle tecnologie dell'informazione e della comunicazione per organizzare la propria attività amministrativa, l'Ente predilige la formazione, gestione, e trasmissione dei documenti in formato nativo digitale.

Per agevolare il processo di formazione dei documenti informatici e favorire, al tempo stesso, la trattazione automatica dei dati in essi contenuti, l'Ente rende disponibili per via telematica moduli e formulari.

Ciò premesso, il documento amministrativo va distinto in:

Documento analogico

Documento informatico

3.2 Formazione dei documenti

I documenti, indipendentemente dalla forma nella quale sono redatti, devono sempre riportare gli elementi essenziali (elencati di seguito).

Dev'essere curata, per quanto possibile, la standardizzazione della forma e dei contenuti dei documenti.

Elementi informativi essenziali dei documenti prodotti

I documenti in uscita devono riportare le seguenti informazioni, organizzate per blocchi logici:

Individuazione dell'autore del documento:

- logo dell'Ente e dicitura "Ordine dei Medici Chirurghi e degli Odontoiatri della Provincia di Campobasso" nelle forme stabilite dall'Ente
- indirizzo completo (via/piazza, numero civico, CAP, città);
- numero di telefono;
- indirizzo istituzionale di posta elettronica;
- indirizzo istituzionale di posta elettronica certificata;

Individuazione e descrizione del documento:

- data ricavata dalla firma digitale;
- numero e descrizione degli allegati;
- numero e data del documento cui si risponde, se necessario;
- oggetto del documento;

Individuazione del destinatario del documento:

- cognome e nome (per le persone), denominazione (per gli enti e le imprese);

e a seconda dei casi:

- indirizzo completo (via/piazza, numero civico, CAP, città);
- indirizzo informatico (PEC, …);

Individuazione del Responsabile del Procedimento Amministrativo[2] (RPA):

- cognome, nome e qualifica del Responsabile del Procedimento Amministrativo;
- firma digitale del RPA;

Individuazione del Responsabile dell'istruttoria:

- cognome e nome del responsabile;
- eventuali dati di contatto.

Formazione dei documenti - aspetti operativi generali

I documenti e i fascicoli dell'Ente sono prodotti con adeguati sistemi informatici e solo in casi eccezionali in modalità analogica.

Ogni documento tratta un unico argomento indicato in maniera sintetica ma esaustiva a cura dell'autore nello spazio riservato all'oggetto, è riferito ad un solo protocollo ed è riconducibile almeno ad un fascicolo o ad un'aggregazione documentaria.

3.3 Formazione del documento analogico

Per documento analogico si intende la rappresentazione non informatica di atti, fatti, o dati giuridicamente rilevanti.

Si definisce "originale" il documento nella sua redazione definitiva corredato degli aspetti diplomatistici sopra descritti.

Un documento analogico può essere convertito in documento informatico corredato da firma digitale ed eventuale attestazione di conformità ai sensi dell'art. 22 del D.lgs. 82/2005 e delle Linee Guida AGID vigenti.

3.4 Formazione del documento informatico

Per documento informatico si intende la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.

Gli atti formati dall'Ente con strumenti informatici, nonché i dati e i documenti informatici detenuti dallo stesso, costituiscono informazione primaria e originale da cui è possibile effettuare, su diversi o identici tipi di supporto, duplicazioni e copie per gli usi consentiti dalla legge.

Il documento informatico è formato mediante una delle seguenti modalità:

- creazione tramite l'utilizzo di strumenti software o servizi cloud qualificati che assicurino la produzione di documenti nei formati e nel rispetto delle regole di interoperabilità di cui all'allegato 2 delle linee guida AGID;
- acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico;
- memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;
- generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica.

Il documento informatico viene identificato in modo univoco e persistente mediante registrazione di protocollo univocamente associata al documento con contestuale generazione dell'impronta crittografica basata su funzioni di Hash che siano ritenute crittograficamente sicure, e conformi alle tipologie di algoritmi previsti nell'allegato 6 delle linee guida nella tabella 1 del paragrafo 2.2 regole di processamento.

L'identificazione dei documenti non protocollati è affidata alle funzioni del sistema di gestione informatica dei documenti che prevede la generazione dell'impronta crittografata come descritto nel paragrafo precedente.

Le caratteristiche di immodificabilità e di integrità sono determinate da una o più delle seguenti operazioni:

- apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata;
- memorizzazione su sistemi di protocollo e gestione documentale che adottino idonee politiche di sicurezza.

Al documento informatico immodificabile vengono associati i metadati che sono stati generati durante l'inserimento nel sistema di gestione documentale. L'insieme minimo dei metadati è costituito da:

- numero di protocollo
- data di protocollo
- oggetto
- mittente – destinatari
- data e protocollo del documento ricevuto, se disponibili
- impronta del documento informatico
- numero degli allegati

[2] In conformità alla Legge 241/90

- classe documentale

3.5 La firma elettronica (avanzata, qualificata, digitale, automatica) e la validazione temporale

La sottoscrizione dei documenti informatici è ottenuta con processi di firma elettronica conformi alle disposizioni dettate dalla normativa vigente.

Per l'apposizione della firma digitale, l'Ente si avvale dei servizi di un'autorità di certificazione iscritta nell'elenco pubblico dei certificatori qualificati tenuto dall'Agenzia per la Cybersicurezza Nazionale (ACN).

I documenti informatici prodotti dall'Ente, indipendentemente dal software utilizzato per la loro redazione, prima della sottoscrizione con firma digitale eseguita al fine di garantirne l'immodificabilità e la corretta archiviazione, sono convertiti nei formati standard previsti dalla norma indicati nell'***Allegato 11 - Formati di file e riversamento dell'Ente***.

La firma digitale viene utilizzata dall'Ente come forma di sottoscrizione per garantire i requisiti di integrità, riservatezza e non ripudiabilità nei confronti di entità esterne e viene apposta prima della protocollazione del documento.

La verifica della firma digitale dei documenti prodotti o ricevuti avviene attraverso verifica manuale dell'operatore o specifiche funzioni integrate nel software di protocollo/gestione documentale nel rispetto della normativa vigente.

3.5.1 La Firma Elettronica Remota Automatica Massiva (FERAM)

Qualora fosse richiesta la firma dei documenti da conferire in conservazione o per la firma di documenti generati automaticamente, questa viene apposta in forma automatica dal software di gestione documentale a mezzo **Firma elettronica remota automatica massiva.**

Si tratta di una particolare tipologia di firma, che rientra nella qualifica di "firma forte"[3], utilizzata in tutti i casi nei quali vi sia il trattamento automatico di grandi quantità di documenti, da ottenere quindi automaticamente e senza presidio.

Al fine di garantire la sicurezza del sistema, il software di protocollo adotta il seguente schema:

- Il RSP può delegare altro utente del protocollo per firmare a suo nome il registro giornaliero di protocollo
- solo l'utente abilitato può inserire le credenziali di firma all'interno della sua area amministrativa.
- le credenziali di cui al precedente punto sono criptate al momento dell'inserimento.

"IrideDoc - Protocollo Informatico, Gestione Documentale e Conservazione Digitale" consente la firma remota automatica anche su un singolo documento.

3.6 La validazione temporale

Per tutte le casistiche per cui la normativa prevede l'apposizione di un riferimento o validazione temporale, l'Ente adotta almeno una delle seguenti modalità di marcatura:

- registrazione di protocollo
- posta elettronica certificata (PEC)
- eventuale sistema di marcatura temporale, nei casi in cui non sia possibile utilizzare uno di quelli precedenti

3.7 Tipologie di formato del documento informatico

L'Ente, in considerazione di quanto previsto dalle linee guida Agid del maggio 2021 in materia di conservazione (e successive modificazioni ed integrazioni), al fine di garantire le caratteristiche di apertura, sicurezza, portabilità, funzionalità, supporto allo sviluppo e diffusione, tende verso l'applicazione delle Linee guida sulla formazione, gestione e conservazione dei documenti informatici emanata da AGID (allegato 2 – Formati di file e riversamento).

L'Ente gestisce esclusivamente formati di file indicati nell'***Allegato 11- Formati di file e riversamento dell'Ente.***

I file compressi devono contenere esclusivamente file con formato incluso nell'allegato di cui sopra.
La scelta dei formati è stata effettuata considerando che essa, come da previsione normativa, deve garantire la leggibilità e la reperibilità del documento informatico nell'intero ciclo di vita dello stesso.
Eventuali integrazioni all'elenco presente nell'allegato sono definite in considerazione di specifiche previsioni normative o tecniche.

Nel caso pervengano documenti su formati diversi da quelli elencati l'Ente avrà cura di avvisare il soggetto produttore in modo da permettere un nuovo invio con formato tra quelli previsti

oppure

qualora il soggetto produttore non ne sia in grado entro il termine richiesto, l'Ente provvede ad effettuare una copia del documento informatico come previsto dal paragrafo 2.3 delle Linee Guida AGID 2021 secondo il seguente schema:

- convertire il documento in uno dei formati adottati ed indicati nell'allegato 11, verificando che vengano mantenuti inalterati i contenuti;
- apporre la firma digitale dell'operatore che intende attestare la conformità della copia all'originale.

3.8 Documenti contenenti collegamenti ipertestuali

Nel caso pervengano documenti contenenti collegamenti ipertestuali (link) a pagine web o file in qualsiasi formato, il servizio gestione documentale avrà cura di avvisare il soggetto produttore affinché provveda ad un nuovo invio, inserendo in allegato (in formato consentito) i file e/o la stampa in formato PDF delle pagine web di destinazione dei collegamenti ipertestuali.

[3] Fonte documenti Namirial

3.9 Documenti contenenti video o audio o social

Nel caso pervengano documenti contenenti video, audio o riferimenti a link a social media, il servizio gestione documentale avrà cura di estrapolare l'impronta Hash degli stessi indicando - in una dichiarazione sostitutiva allegata al protocollo – che la sequenza di bit, detta digest (o stringa) è strettamente correlata ai dati in ingresso.

4. FLUSSI DI LAVORAZIONE DEI DOCUMENTI

II presente capitolo fornisce indicazioni sulle modalità di lavorazione dei documenti ricevuti e prodotti dall'Ente.

Nell'ambito del processo di gestione documentale, il documento amministrativo, in termini operativi, è così classificabile:

- ricevuto
- inviato

Secondo quanto previsto dall'art. 40 del decreto legislativo n. 82/2005 "*le pubbliche amministrazioni che dispongono di idonee risorse tecnologiche formano gli originali dei propri documenti con mezzi informatici secondo le disposizioni di cui al presente codice e le regole tecniche"* e successive Linee Guida Agid.

La redazione di documenti originali su supporto cartaceo, nonché la copia di documenti informatici sul medesimo supporto è consentita solo ove risulti necessaria e comunque nel rispetto del principio dell'economicità.

Pertanto, il documento amministrativo può essere disponibile anche nella forma analogica nei casi previsti dalla legge.

4.1 Documenti in entrata

La corrispondenza in ingresso può essere acquisita dall'Ente con diversi mezzi e modalità in base alla tecnologia di trasporto utilizzata dal mittente.

4.1.2 Ricevuti o prodotti su supporto analogico

I documenti ricevuti su supporto analogico possono essere recapitati attraverso:

- a mezzo posta convenzionale, corriere o telegramma
- a mezzo posta raccomandata
- brevi manu

4.1.3 Ricevuti o prodotti su supporto informatico

I documenti informatici possono essere recapitati/trasmessi tramite: posta elettronica convenzionale o certificata (la casella mail istituzionale dell'Ente, casella PEC dell'Ente (…), pubblicate sul sito istituzionale https://www.ordinedeimedici.cb.it/, su supporto rimovibile quale, ad esempio, cd rom, dvd, pen-drive, consegnato direttamente al SGD o inviato per posta convenzionale o corriere.

4.2 Documenti in uscita

La trasmissione dei documenti in uscita avviene in via prioritaria mediante l'uso dei canali informatici a meno che il destinatario non richieda motivandola una modalità diversa.

Inviati su supporto analogico

I documenti analogici sono trasmessi attraverso:

- servizi postali
- brevi manu
- notifica atti

Inviati su supporto informatico

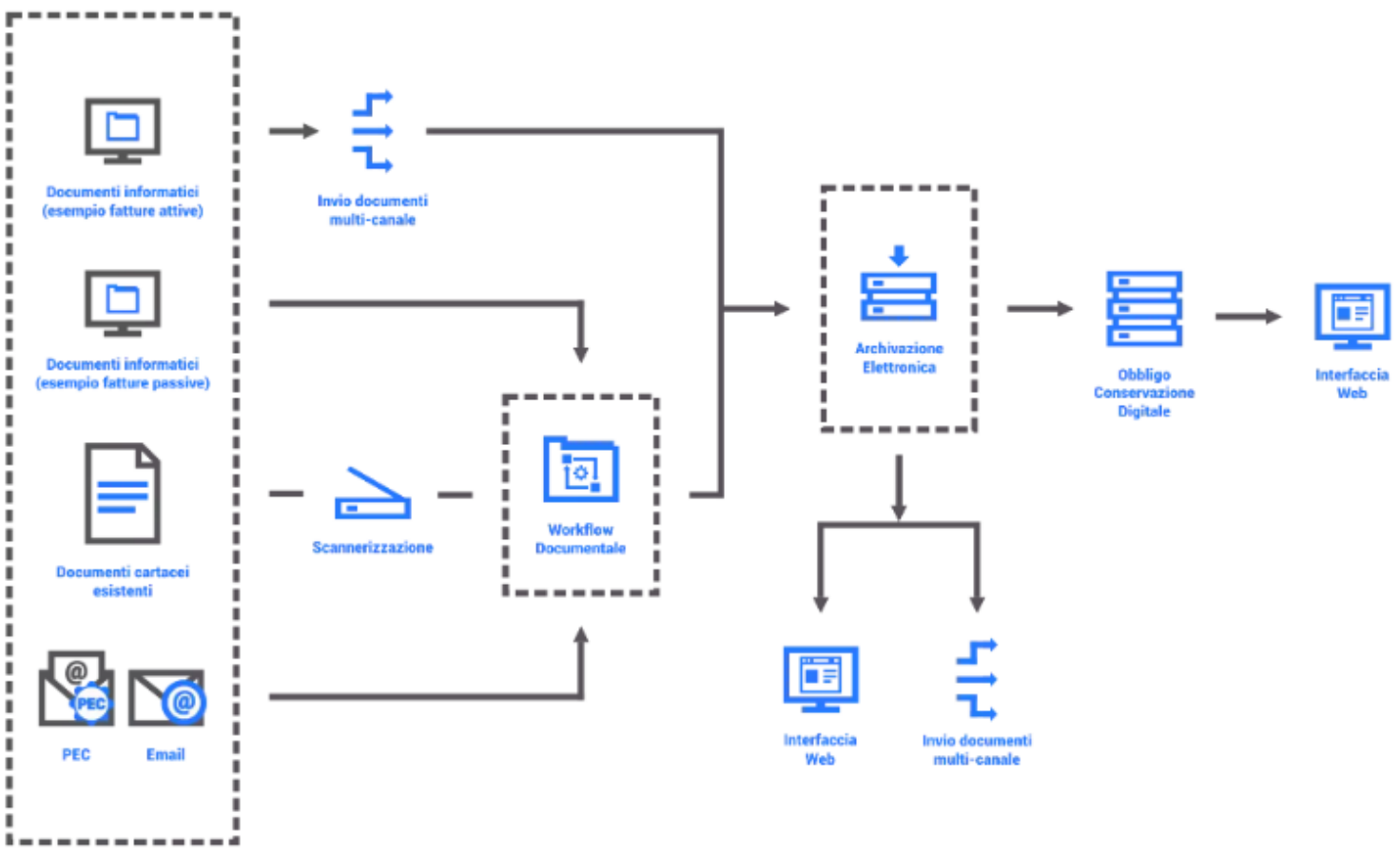
I documenti informatici sono trasmessi attraverso:

- posta elettronica certificata (PEC)
- flussi informatici
- caselle di posta elettronica

Solo la trasmissione dalla casella di PEC istituzionale ad una casella PEC del destinatario costituisce, infatti, evidenza giuridico-probatoria dell'invio e della consegna del messaggio (art. 47 CAD).

4.3 Descrizione del flusso di lavorazione dei documenti

Il presente capitolo rappresenta graficamente il diagramma dei flussi per la gestione in entrata ed in uscita dei documenti ricevuti e spediti dall'Ente:



5. MODALITÀ DI PRODUZIONE E DI CONSERVAZIONE DELLE REGISTRAZIONI DI PROTOCOLLO INFORMATICO

Il presente capitolo illustra le modalità di produzione e di conservazione delle registrazioni di protocollo informatico, nonché le modalità di registrazione delle informazioni annullate o modificate nell'ambito di ogni sessione di attività di registrazione.

L'Ente utilizza il sistema di protocollo informatico e di gestione documentale indicato al cap. 1.6.

5.1 Registrazione dei documenti

Tutti i documenti dell'Ente, con particolare riferimento a quei documenti dai quali possano nascere diritti, doveri o legittime aspettative di terzi, devono essere registrati sul protocollo informatico unico dell'Ente, con le modalità e le eccezioni di seguito illustrate.

La registrazione è l'operazione di memorizzazione delle informazioni fondamentali previste dalla normativa vigente.

Tale operazione serve a identificare in modo univoco un documento individuandone data, forma e provenienza certa.

Anche i documenti soggetti a repertoriazione, forma particolare di registrazione, vengono registrati sul protocollo informatico unico dell'Ente.

La registrazione di protocollo riguarda il singolo documento; non può riguardare per alcun motivo il fascicolo. Quindi il numero di protocollo individua un singolo documento.

I documenti sono poi raccolti in fascicoli informatici o ibridi o in aggregazioni documentali per tipologie di documenti (serie).

5.1.2 Modalità di registrazione di protocollo

Per registrazione di protocollo si intende l'apposizione o l'associazione al documento, in forma permanente e non modificabile, delle informazioni riguardanti il documento stesso.

La registrazione si effettua di norma entro la giornata di arrivo o comunque entro 24 ore lavorative dal ricevimento o, se intercorrono dei giorni festivi o di chiusura programmata dell'Ente, nel primo giorno lavorativo utile.

Il Protocollo generale provvede all'apertura della corrispondenza e a separare i documenti esclusi dalla registrazione di protocollo ***(Allegato 12 - Documenti esclusi dalla registrazione di Protocollo)***

Nell'ambito dell'Ente, il registro di protocollo è unico e la sua numerazione progressiva è costituita da 7 cifre numeriche, si chiude al 31 dicembre di ogni anno e ricomincia dal primo gennaio dell'anno successivo.

Il numero di protocollo individua un unico documento principale ed eventuali allegati e, di conseguenza, ogni documento con i relativi allegati reca un solo numero di protocollo immodificabile.

Contestualmente alla registrazione i documenti analogici vengono sempre acquisiti nel sistema di protocollo tramite procedura di scansione.

Nel caso di ricezione dello stesso documento da parte di più destinatari interni all'Ente occorre evitare una molteplice registrazione dello stesso documento.

Il registro di protocollo è un atto pubblico originario che fa fede della tempestività e dell'effettivo ricevimento e spedizione di un documento, indipendentemente dalla regolarità del documento stesso, ed è idoneo a produrre effetti giuridici.

Tutti i documenti analogici in entrata o in uscita registrati devono essere acquisiti in copia per immagine e associati alla registrazione di protocollo.
Fanno eccezione i documenti che materialmente non possono essere sottoposti a scansione (a titolo meramente esemplificativo: volumi, registri, plichi, planimetrie di formato superiore all'A3, plastici, monete, ecc.) che devono essere elencati e descritti in un documento che verrà acquisito come documento principale.

5.1.3 Documento analogico inviato elettronicamente

Se il documento analogico è inviato tramite posta elettronica certificata o canali digitali, viene gestito come segue:

- redatto in un unico esemplare
- sottoscritto con firma autografa
- acquisito tramite scansione nel sistema di protocollo
- firmato digitalmente dall'operatore di protocollo, il quale provvederà anche ad apporre l'attestazione di conformità
- associato al protocollo stesso e al fascicolo relativo

L'operatore provvede poi all'invio del file all'indirizzo telematico del destinatario.
Viene quindi conservato presso l'Ente e inserito nel fascicolo.

Documento digitale inviato elettronicamente

Se il documento digitale è inviato tramite posta elettronica certificata o canali digitali, viene gestito come segue:

- redatto tramite un software adeguato (es. elaborazione testi)
- sottoscritto con firma digitale
- acquisito nel sistema di protocollo
- associato al protocollo stesso e al fascicolo relativo

L'operatore provvede poi all'invio del file all'indirizzo telematico del destinatario.

5.2 Registri di protocollo periodici

Il registro di protocollo è un documento informatico prodotto e redatto secondo le modalità previste dalla vigente normativa.

Invio in conservazione del registro giornaliero di protocollo

Il registro di protocollo giornaliero riporta tutti i protocolli generati nell'arco della singola giornata.

Il "registro di protocollo"[4] ricomprendere i metadati minimi indicati nell'allegato 5 delle Linee Guida AGID 2021 ma anche gli ulteriori metadati indicati nella circolare AGID art. 53, comma 1, del DPR 445/2000 e dalla Circolare AGID n. 60 del 2013.

- anno
- numero della prima registrazione effettuata sul registro
- numero dell'ultima registrazione effettuata sul registro
- data della prima registrazione effettuata sul registro
- data dell'ultima registrazione effettuata sul registro

In particolare, la registrazione di protocollo per ogni documento ricevuto o spedito richiede la memorizzazione delle seguenti informazioni:

- il numero di protocollo del documento
- la data di registrazione di protocollo
- il mittente o i destinatari
- l'oggetto del documento
- l'impronta del documento principale
- indicazione del registro di protocollo

Il registro giornaliero di protocollo contiene quindi, in modo ordinato e progressivo, l'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno ed è soggetto alle forme di pubblicità e di tutela di situazioni giuridicamente rilevanti previste dalla normativa vigente.

Ai sensi dell'art. 7 comma 5 del DPCM 3 dicembre 2013, il registro giornaliero di protocollo viene firmato digitalmente dal responsabile del protocollo e trasmesso entro la giornata lavorativa successiva al sistema di conservazione, garantendone l'immodificabilità del contenuto.

[4] Conformemente anche a quanto indicato nel documento AGID "PRODUZIONE E CONSERVAZIONE DEL REGISTRO GIORNALIERO DI PROTOCOLLO"
https://www.agid.gov.it/sites/default/files/repository_files/documenti_indirizzo/istruzioni_per_la_produzione_e_conservazione_registro_giornaliero_di_protocollo.pdf

Oltre al registro giornaliero di protocollo è previsto l'invio in conservazione del registro dei protocolli sia mensile (entro 7 giorni lavorativi dalla fine del mese precedente) che annuale (entro il 31 gennaio dell'anno successivo) dei protocolli.

Questo al fine di riportare nei registri le eventuali variazioni intercorse.

5.3 La segnatura di protocollo

La segnatura di protocollo avviene contemporaneamente all'operazione di registrazione mediante l'apposizione o l'associazione all'originale del documento, in forma permanente e non modificabile, delle informazioni riguardanti il documento stesso. Essa consente di individuare ciascun documento in modo inequivocabile.

Le informazioni necessarie sono indicate all'interno dell'allegato 6 "Comunicazioni tra AOO di documenti amministrativi protocollati" delle linee guida AgID sulla formazione, gestione e conservazione dei documenti informatici.

Quando il documento è indirizzato ad altre amministrazioni ed è sottoscritto con firma digitale e trasmesso con strumenti informatici, la segnatura di protocollo può includere le informazioni di registrazione del documento purché siano adottate idonee modalità di formazione dello stesso in formato pdf (preferibilmente pdf/a).

Qualora il documento venga prodotto su formato analogico, al termine della registrazione, la segnatura viene apposta direttamente sul supporto cartaceo tramite timbro o etichetta (le cui informazioni sono il risultato dell'estrazione delle informazioni minime contenute nella segnatura informatica). Questa riporterà il numero e la data di protocollo.

Qualora il documento venga prodotto in formato nativo digitale il numero di protocollo è indicato:

- nel nome del file
- nell'oggetto della mail nel caso di trasmissione con posta elettronica
- nel file di segnatura in formato xml nel caso di trasmissione con posta elettronica

5.4 Procedure specifiche nella registrazione di protocollo

5.4.1 Protocollazione di documenti riservati

I documenti di carattere riservato sono trattati esclusivamente dal personale autorizzato.

I documenti vengono caricati nel sistema di gestione documentale e vengono poi protocollati e classificati in modo da garantirne la condizione di riservatezza.

Tale accesso può essere esteso anche a cariche istituzionali dell'Ente (es. presidente, consiglieri, ecc.) purché ne abbiano facoltà.

5.4.2 Modifica della gestione della sicurezza per documenti classificati come "riservati"

Il RSP monitora periodicamente l'adeguatezza del sistema organizzativo e del software utilizzato per la registrazione di protocollo e gestione documentale. Particolare riguardo viene concesso agli aspetti della sicurezza e riservatezza.

Le tipologie di documenti da registrare nel protocollo riservato saranno codificate all'interno del sistema di protocollo informatico a cura del responsabile del Servizio archivistico dell'Ordine, di concerto con il responsabile amministrativo dell'Ordine. Le procedure adottate per la gestione dei documenti e dei procedimenti amministrativi ad accesso riservato, comprese la registrazione, la segnatura, la classificazione e la fascicolazione, saranno le stesse adottate per gli altri documenti e procedimenti amministrativi.

Il sistema può associare il livello di riservatezza in relazione alla classe documentale assegnata al protocollo/documento.

Il Responsabile del servizio archivistico o un suo delegato che effettua l'operazione di apertura di un nuovo fascicolo può stabilire anche il livello di riservatezza applicando, tramite le apposite funzioni, le autorizzazioni a livello di ruolo oppure di singolo utente.

Il livello di riservatezza applicato ad un fascicolo è acquisito automaticamente da tutti i documenti che vi confluiscono, se a questi sia stato assegnato un livello di riservatezza minore o uguale. I documenti che invece hanno un livello di riservatezza superiore lo mantengono.

Per approfondimenti su altri aspetti di riservatezza e privacy vedere capitolo 2.

5.4.3 Documenti esclusi dalla registrazione di protocollo

Il DPR 445/2000 prevede che tutti i documenti in entrata e in uscita e tutti i documenti informatici siano registrati a protocollo, con alcune eccezioni di cui all'allegato ***(Allegato 12 - Documenti esclusi dalla registrazione di Protocollo).***

5.4.4 Modifica delle registrazioni di protocollo

Le uniche informazioni modificabili della registrazione di protocollo sono la classe documentale e l'assegnazione.

Tali modifiche vengono storicizzate e rese visibili e comparabili ai sensi dell'art. 54 del DPR 445/2000 e ss.mm.ii.

5.4.5 Annullamento delle registrazioni di protocollo

La procedura di annullamento di una registrazione è di competenza del Responsabile del servizio archivistico o del suo delegato.

L'annullamento della registrazione di protocollo prevede la memorizzazione dei seguenti dati:

- data di annullamento
- operatore
- motivo dell'annullamento

Tali modifiche vengono storicizzate e rese visibili e comparabili ai sensi dell'art. 54 del DPR 445/2000 e ss.mm.ii.

5.5 Casi particolari di registrazioni di protocollo

5.5.1 Lettere anonime

La lettera anonima, una volta aperta e attestata l'assenza di ogni riferimento al mittente, viene posta all'attenzione del Segretario/Responsabile amministrativo o di persona dallo stesso delegata, che fornirà istruzioni in merito al suo trattamento agli addetti del Protocollo, i quali provvederanno secondo le indicazioni ricevute, alla sua registrazione (indicando nel campo mittente "anonimo") ovvero alla sua eliminazione.

5.5.2 Documenti privi di firma

I documenti con mittente, privi di firma, vanno protocollati. La funzione notarile del protocollo (cioè, della registrazione) è quella di attestare data e provenienza certa di un documento senza interferire su di esso.

5.5.3 Corrispondenza personale o riservata

La corrispondenza personale (es. Mario Rossi c/o Ordine dei Medici …) è regolarmente aperta dagli uffici incaricati della registrazione di protocollo dei documenti in arrivo, a meno che sulla busta non sia riportata la dicitura "riservata" o "personale" o "s.p.m".

In quest'ultimi casi, la corrispondenza non è aperta ed è consegnata al destinatario, il quale, dopo averne preso visione, se reputa che i documenti ricevuti debbano essere comunque protocollati provvede a trasmetterli all'ufficio abilitato alla registrazione di protocollo.

5.5.4 Integrazioni documentarie

L'addetto al protocollo non è tenuto a controllare la completezza formale e sostanziale della documentazione pervenuta, ma è tenuto a registrare in ogni caso il documento ed eventuali allegati.

Tale verifica spetta al Responsabile del Procedimento Amministrativo (RPA) che, qualora reputi necessario acquisire documenti che integrino quelli già pervenuti, provvede a richiederli al mittente.

I documenti pervenuti ad integrazione di quelli già disponibili sono protocollati oppure integrati come documenti secondari nella registrazione di protocollo originaria e sono inseriti nel fascicolo relativo.

5.5.5 Documenti pervenuti per errore all'Ente

I documenti pervenuti per errore all'Ente non devono essere protocollati e devono essere spediti immediatamente al mittente con la dicitura «Erroneamente pervenuto all'Ordine dei Medici Chirurghi e degli Odontoiatri di (…) il (giorno.mese.anno)».

5.5.6 Trattamento dei documenti con oggetto o smistamento plurimo

Ogni documento, anche se in più esemplari, deve essere individuato da un solo e unico numero di protocollo, indipendentemente dal fatto che sia indirizzato, per competenza o per conoscenza, a una o più strutture amministrative e/o organi politici all'interno dell'Ente. Di conseguenza, qualora pervenga un documento nel quale risultano evidenti più destinatari, l'addetto alla registrazione, prima di protocollarlo, deve verificare, attraverso il sistema informatico, che esso non sia già stato registrato dagli altri destinatari.

Nel caso in cui, oltre alla pluralità di destinatari, il documento tratti anche una pluralità di argomenti (pluralità di oggetti), afferenti a procedimenti diversi e – conseguentemente – a fascicoli diversi, si individua la classe principale e si inserisce nei relativi fascicoli da cui ne ereditano la classe.

Ogni documento in uscita deve obbligatoriamente trattare un solo oggetto (un solo argomento) e deve necessariamente riferirsi ad un solo procedimento.

5.5.7 Documenti in partenza con più destinatari

Qualora i destinatari del documento siano molteplici nella registrazione di protocollo, questi vanno tutti riportati nel campo "destinatario".

Solo in casi eccezionali e qualora i destinatari siano in numero superiore a 10, si utilizza uno dei destinatari particolari, esempio: "TUTTI GLI ISCRITTI".

Al fine di permettere una corretta protocollazione, nei casi di invio massivo di un documento ed utilizzo dei "destinatari particolari", l'Ufficio di protocollo associa come documento secondario del protocollo un file contenente l'elenco dei destinatari individuati con nome, cognome o Ragione Sociale, codice fiscale e il recapito.

Nel caso di invio di comunicazioni massive quando il documento è identico questo sarà il documento principale del protocollo, nel caso in cui il documento è personalizzato il documento principale sarà il modello definito per la generazione dei singoli file personalizzati.

5.5.8 Flussi documentali informatici

5.5.8.1 Flusso FNOMCeO-ENPAM

L'Ente è tenuto periodicamente all'invio delle posizioni degli iscritti alla FNOMCeO e all'ENPAM. Tale invio avviene con una procedura semiautomatica:

- generazione a partire dal gestionale Albi di 2 file in formato xml
- verifica della correttezza formale dei file
- protocollazione del file "Anagrafica" indicando come destinatari FNOMCeO ed ENPAM
- protocollazione del file "Datifnom" indicando come destinatario FNOMCeO

I due file vengono inviati tramite il software fornito da FNOMCeO e ENPAM.

5.5.8.2 Flusso OIL (ordinativo informatico)

Anche in questo caso viene generato un flusso xml dall'applicativo *ContoTecsis*, software di contabilità pubblica per Enti Pubblici non Economici, coerente con DPR 696/79 e DPR 97/2003, che viene poi firmato digitalmente da Presidente, Segretario e Tesoriere, quindi protocollato e infine inviato telematicamente alla banca che funge da Cassiere/Tesoriere. *ContoTecsis* ha un connettore integrato che permette, secondo i principi dell'interoperabilità, di inviare i dati dei pagamenti al portale RgS per ottemperare a quanto previsto dalla normativa

5.5.8.3 Fatture elettroniche

Le fatture elettroniche e le notifiche vengono protocollate con una procedura automatica che giornalmente, per mezzo di un job eseguito dal server in orario serale, le riversa nel software del protocollo inserendo i seguenti metadati:

- numero e data protocollo
- data riferimento del documento: viene impostata la data di emissione della fattura
- oggetto: viene composto secondo uno standard predefinito - fatt. [num fattura] del [data emissione] emessa da [ragione sociale fornitore e partita iva]
- classe documentale per le fatture e per le notifiche
- direzione: entrata
- mittente: viene caricato il soggetto corrispondente sulla base del codice fiscale inserito nell'anagrafica o, se non presente, viene anche anagrafato il soggetto
- mezzo di trasmissione: quello configurato nel software di protocollo per questa tipologia di documenti
- documento primario: fattura elettronica
- documento secondario: metadati allegati alla fattura

5.5.8.4 Istanze telematiche

Le istanze telematiche (domanda di prima iscrizione e domanda di cancellazione) vengono protocollate dall'operatore per mezzo di un connettore presente nel software di protocollo che recupera i dati direttamente dall'istanza effettuata in cloud.

L'operatore dovrà quindi solo dare l'input di protocollazione ed il software provvederà a protocollare la singola istanza impostando automaticamente i seguenti dati:

- numero e data protocollo
- data riferimento del documento: viene impostata la data di invio dell'istanza
- oggetto: viene composto secondo uno standard predefinito - domanda prima iscrizione all'Albo…..del dott. x y, c.f. …..; domanda di cancellazione dall'albo….del dott. xy, c.f. ……
- classe documentale per le istanze di prima iscrizione e cancellazione albo medici e per le istanze di prima iscrizione e cancellazione albo odontoiatri
- direzione: entrata
- mittente: viene caricato il soggetto corrispondente sulla base del codice fiscale inserito nell'anagrafica o, se non presente, viene anche anagrafato il soggetto
- mezzo di trasmissione: quello configurato nel software di protocollo per questa tipologia di documenti
- documento primario: istanza telematica
- documento secondario: eventuali allegati all'istanza (a titolo esemplificativo documento d'identità, ricevute di pagamento, ecc)

5.6 Regole di smistamento e di assegnazione

L'operazione di smistamento consiste, da parte dell'operatore di protocollo, nell'assegnazione al personale addetto all'attività preposta.
Si adottano le modalità operative di seguito illustrate:

- quotidianamente gli operatori e/o i responsabili verificano i documenti a loro assegnati;
- ogni soggetto provvede alla visione e alla gestione del documento assegnato e alla sua eventuale riassegnazione ad altro collega.

5.6.1 Processo di assegnazione dei fascicoli

Quando un nuovo documento viene formato o ricevuto dall'amministrazione, il responsabile del procedimento o suo delegato abilitato all'operazione di fascicolazione stabilisce, con l'ausilio delle funzioni di ricerca del sistema di protocollo informatizzato, se il documento stesso debba essere inserito in un fascicolo già esistente, oppure sia necessario aprire un nuovo fascicolo.

A seconda delle ipotesi, si procede come segue:

Se il documento si riferisce a un fascicolo aperto, l'addetto:
- seleziona il relativo fascicolo
- collega la registrazione di protocollo del documento al fascicolo selezionato (se si tratta di un documento su supporto cartaceo, assicura l'inserimento fisico dello stesso nel relativo fascicolo cartaceo)

Se il documento non è riferito ad alcun fascicolo aperto, il soggetto preposto:
- esegue l'operazione di apertura del fascicolo sulla base del piano di fascicolazione (Allegato n. 7)
- collega la registrazione di protocollo del documento al fascicolo appena creato

6. MODALITÀ DI UTILIZZO DEL REGISTRO DI EMERGENZA

Nelle situazioni di emergenza nelle quali non sia possibile utilizzare il protocollo informatico, ogni documento in entrata o in uscita deve essere registrato su un supporto alternativo, denominato Registro di emergenza (***Allegato 13: Modello del Registro di emergenza***).

Per emergenza si intende una situazione in cui la sospensione del servizio si protragga oltre le **8 ore** o che sia comunque tale da pregiudicare la registrazione a protocollo in giornata, nel caso in cui vi siano scadenze inderogabili e prescrittive (es: bandi, concorsi, ecc.).

L'utilizzo del registro di emergenza deve essere autorizzato dal RSP o suo delegato come descritto al cap. 1.5.

Per la registrazione di emergenza si utilizza:

nel caso di disponibilità dei PC un modulo in formato Excel disponibile tra la modulistica amministrativa dell'Ente; il modulo potrà essere compilato mediante l'immissione dei dati direttamente sulla tabella

nel caso di impossibilità ad utilizzare i PC ci si avvarrà del modulo cartaceo di cui al fac simile allegato al Manuale di gestione che verrà compilato manualmente

Sul registro di emergenza devono essere riportate la causa, la data e l'ora di inizio dell'interruzione, la data e l'ora di ripristino della piena funzionalità del sistema, nonché eventuali note ritenute rilevanti dal responsabile del protocollo informatico e della gestione documentale.

Prima di autorizzare l'avvio della procedura, il RSP deve impostare e verificare la correttezza di data e ora sui rispettivi registri di emergenza. In caso di vicinanza alla data di fine anno solare, si tenga presente che ogni registro di emergenza si rinnova ogni anno solare.

Ogni documento è individuato dal numero assegnato nel Registro di emergenza, anno di registrazione, numero di protocollo nel formato stabilito; ad esempio:

RE01-2023-0000005.

Una volta ripristinata la piena funzionalità del sistema, il RSP provvede alla chiusura dei registri di emergenza, annotando su ciascuno il numero di registrazioni effettuate e la data e ora di chiusura e dovrà protocollare il registro di emergenza attivato.

I dati delle registrazioni di emergenza dovranno essere inseriti nel sistema informatico di protocollo e si configurano come un repertorio dello stesso.

Ad ogni registrazione recuperata dal registro di emergenza sarà attribuito un nuovo numero di protocollo, seguendo senza soluzione di continuità la numerazione del protocollo informatico unico raggiunta al momento dell'interruzione del servizio. A tale registrazione sarà associato anche il numero di protocollo e la data di registrazione del relativo protocollo di emergenza.

I documenti annotati nel registro di emergenza e trasferiti nel protocollo informatico unico recheranno, pertanto, due numeri: uno del protocollo di emergenza e uno del protocollo informatico unico. Al numero e data attribuiti dal registro di emergenza si fa riferimento per l'avvio dei termini del procedimento amministrativo.

7. SISTEMA DI CLASSIFICAZIONE, FASCICOLAZIONE E PIANO DI CONSERVAZIONE

7.1 Protezione e conservazione degli archivi pubblici

Gli archivi e i singoli documenti degli Enti Pubblici sono beni culturali inalienabili ai sensi dell'art. 10, comma 2 del Decreto legislativo 42/2004.

Quindi, tutti i documenti acquisiti e prodotti nel sistema di gestione documentale dall'Ente, sono inalienabili e appartengono ad un unico complesso archivistico, che è l'archivio dell'Ente.

L'archivio non può essere smembrato e dev'essere conservato nella sua organicità. Lo scarto dei documenti, siano essi cartacei o informatici, è subordinato all'autorizzazione della Soprintendenza archivistica competente per la regione di appartenenza ai sensi degli artt. 20 e 21 del Decreto legislativo 42/2004.

Per l'archiviazione e la custodia nella sezione di deposito, o storica, dei documenti contenenti dati personali, si applicano le disposizioni di legge sulla tutela della riservatezza dei dati personali (GDPR 679/2016 e s.m.i.).

Ai sensi dell'art. 30 del Decreto legislativo 42/2004 ***Codice dei beni culturali e del paesaggio (ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137)***, dell'art. 30 del DPR 30 settembre 1963, n. 1409 ***Norme relative all'ordinamento ed al personale degli archivi di Stato*** e degli artt. 67 e 69 del DPR 445/2000 ***Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa***, L'Ente, in quanto ente pubblico, ha l'obbligo di:

garantire la sicurezza e la conservazione del proprio archivio e procedere al suo ordinamento
costituire uno, o più archivi di deposito nei quali trasferire annualmente i fascicoli relativi agli affari conclusi
istituire una sezione separata d'archivio per i documenti relativi ad affari esauriti da più di 40 anni (archivio storico) e redigere l'inventario degli stessi.

L'archivio è quindi un'entità unitaria, che conosce tre fasi:

archivio corrente[5] : riguarda i documenti necessari alle attività correnti;
archivio di deposito[6]: riguarda i documenti ancora utili per finalità amministrative o giuridiche, ma non più indispensabili per la trattazione delle attività correnti;
archivio storico[7]: riguarda i documenti storici selezionati per la conservazione permanente

[5] In ambito informatico si può assumere che appartengano a questa fase i documenti o fascicoli non chiusi

[6] In ambito informatico si può assumere che appartengano a questa fase i documenti o fascicoli chiusi (indipendentemente dal fatto che siano stati inviati o meno in conservazione digitale)

[7] In ambito informatico si può assumere che appartengano a questa fase tutti i documenti o i fascicoli che, con anzianità superiori ai 40 anni, siano presenti nel sistema di gestione del protocollo informatico a valle di tutte le fasi di sfoltimento avvenute nel tempo.

Il trattamento del sistema documentale dell'Ente implica la predisposizione di strumenti di gestione dell'archivio corrente che consentano un'efficace organizzazione e consultazione della documentazione, a prescindere dai supporti dei documenti.

Il presente capitolo descrive il sistema di classificazione dei documenti, di formazione del fascicolo e di conservazione dell'archivio, con l'indicazione dei tempi e delle modalità di aggiornamento, dei criteri e delle regole di selezione e scarto della documentazione e di consultazione e movimentazione dei fascicoli.

La classificazione dei documenti, destinata a realizzare una corretta organizzazione dell'archivio, è obbligatoria per legge e si avvale del piano di classificazione (Titolario).

Il piano di conservazione, collegato con il Titolario ed elaborato tenendo conto dei flussi documentali dipendenti dai procedimenti e dalle prassi seguiti dall'Ente nell'espletamento delle funzioni istituzionali, definisce i tempi di conservazione dei documenti e dei fascicoli.

Titolario e piano di conservazione, in quanto strumenti che consentono la corretta gestione e conservazione, sono predisposti, verificati e/o confermati antecedentemente all'avvio delle attività di registrazione di protocollo e di archiviazione. Il Titolario e il piano di conservazione sono adottati con atti formali dai vertici dell'amministrazione.

7.2 Titolario o piano di classificazione

7.2.1 Titolario

Il Titolario o Piano di classificazione è un sistema precostituito di partizioni astratte gerarchicamente ordinate, individuato sulla base dell'analisi delle funzioni dell'Ente, al quale viene ricondotta la molteplicità dei documenti prodotti.

L'Ente utilizza un titolario, adottato con deliberazione N. 46/2016 e successive (vedi ***Allegato 5 -Titolario di classificazione***) organizzato a 2 livelli suddiviso in titoli e classi. Il titolo (o la voce di l° livello) individua per lo più funzioni primarie e di organizzazione dell'Ente (macrofunzioni); le successive partizioni (classi) corrispondono a specifiche competenze che rientrano concettualmente nella macrofunzione descritta dal titolo, articolandosi gerarchicamente tra loro in una struttura ad albero rovesciato.

Titoli e classi sono nel numero prestabilito dal titolario di classificazione e non sono modificabili né nel numero né nell'oggetto, se non per provvedimento esplicito del Consiglio Direttivo dell'Ente su proposta del RSP.

L'Ente di norma sottopone il Titolario all'approvazione della Soprintendenza di riferimento.

Dopo ogni modifica del titolario, il RSP provvede ad informare tutti i soggetti abilitati all'operazione di classificazione dei documenti e a dare loro le istruzioni per il corretto utilizzo delle nuove classifiche, le eventuali modifiche e integrazioni entrano in vigore il 1° gennaio dell'anno seguente. Il titolario non è retroattivo: non si applica cioè, ai documenti protocollati prima della sua introduzione.

Il sistema di protocollazione garantisce la storicizzazione delle variazioni di titolario e la possibilità di ricostruire le diverse voci nel tempo, mantenendo stabili i legami dei fascicoli e dei documenti con la struttura del titolario vigente al momento della produzione degli stessi.

Per ogni specifica voce viene riportata la data di inserimento e la data di variazione.

7.2.2 Classificazione dei documenti

La classificazione è l'operazione finalizzata all'organizzazione dei documenti, secondo l'ordinamento del Titolario. Viene effettuata su tutti i documenti ricevuti e prodotti dell'Ente, indipendentemente dal supporto sul quale vengono formati.

La classificazione (apposizione/associazione di titolo e classe al documento) è necessaria e preliminare all'attività di fascicolazione.

Le informazioni relative alla classificazione nei casi dei documenti amministrativi informatici costituiscono parte integrante dei metadati previsti per la formazione dei documenti medesimi.

7.3 Formazione del fascicolo

7.3.1 Il fascicolo

Il fascicolo costituisce l'unità archivistica di base, che permette, nel tempo, la gestione ottimale della documentazione detenuta istituzionalmente da qualsiasi Amministrazione.

Il fascicolo rappresenta una delle unità archivistiche elementari (documento, fascicolo, registro) e può essere definito come "*un insieme organico di documenti raggruppati o dal soggetto produttore per le esigenze della sua attività corrente o nel corso dell'ordinamento dell'archivio, in base al comune riferimento allo stesso oggetto, attività o negozio giuridico*".

I documenti registrati e classificati nel sistema informatico (protocollati) sono riuniti in fascicoli o in aggregazioni documentali.

I fascicoli vengono creati secondo le indicazioni riportate nel piano di fascicolazione (All. 7) dove vengono riportate le tipologie di fascicoli (o l'eventuale gestione in repertori) e l'indicazione se il fascicolo ha durata annuale o per singola attività o procedimento.

I documenti sono archiviati all'interno di ciascun fascicolo secondo l'ordine cronologico di registrazione.

Qualora un documento dia luogo all'avvio di un procedimento amministrativo, il RPA assegnatario del documento stesso, deve provvedere all'apertura (istruzione) di un nuovo fascicolo che comprende la registrazione dei relativi metadati.

Ogni fascicolo è caratterizzato dai seguenti metadati:

- indice di classificazione, (titolo, classe)
- identificativo progressivo
- oggetto del fascicolo
- data di apertura del fascicolo

- data di chiusura
- nominativo del responsabile
- tipologia

7.3.2 Famiglie e tipologie di fascicolo

I fascicoli sono suddivisi in 4 categorie:

- fascicoli inerenti persone fisiche
- fascicoli inerenti persone giuridiche
- fascicoli inerenti procedimenti amministrativi
- fascicoli inerenti affari o attività

Per ogni persona fisica o giuridica deve essere istruito un fascicolo nominativo. Il fascicolo viene generato dall'operatore di protocollo.

L'apertura prevede la registrazione di alcune informazioni essenziali:

- identificativo progressivo
- indice di classificazione
- oggetto del fascicolo
- data di apertura del fascicolo
- nominativo del responsabile del procedimento/fascicolo
- tipologia

I documenti sono archiviati all'interno di ciascun fascicolo, secondo l'ordine cronologico di registrazione, in base cioè al numero di protocollo ad essi attribuito.

Il fascicolo viene chiuso al termine del procedimento amministrativo o all'esaurimento dell'affare/attività. I fascicoli classificati come annuali vengono chiusi alla fine dell'anno solare e possono essere riaperti con modalità automatica per l'anno successivo. La data di chiusura si riferisce alla data dell'ultimo documento prodotto.

Per quanto riguarda i fascicoli di persona questi verranno chiusi nel momento in cui il ruolo giuridico di quella persona viene meno (per es. quando un iscritto si cancella o quando un dipendente cessa l'attività lavorativa).

7.3.3 Repertorio dei fascicoli

Ogni Fascicolo ha un proprio "IDENTIFICATIVO", costituito da un codice che consente di identificare univocamente un'entità dal punto di vista amministrativo. Tale identificativo è strutturato conformemente a quanto indicato nella CIRCOLARE AGID N. 60 DEL 23 GENNAIO 2013 (Pag. 71)[8]

Il repertorio dei fascicoli, ripartito per ciascun titolo del titolario, è lo strumento di gestione e di reperimento dei fascicoli. La struttura del repertorio, quindi, rispecchia quella del titolario di classificazione e varia in concomitanza con l'aggiornamento di quest'ultimo. Mentre il titolario rappresenta in astratto le funzioni e le competenze che l'Ente può esercitare, in base al proprio mandato istituzionale, il repertorio dei fascicoli rappresenta, in concreto, le attività svolte e i documenti prodotti in relazione a tali attività.

Gli elementi costitutivi del repertorio di fascicoli sono:

- l'anno di riferimento
- l'indice di classificazione completo (titolo, classe, sottoclasse, etc.)
- identificativo (es. 2025-0000002)
- la data/anno di apertura
- la data/anno di chiusura
- l'oggetto del fascicolo
- le note sullo stato del fascicolo, cioè se è aperto o chiuso
- eventuali note
- tipologia

7.3.4 Il fascicolo personale dell'iscritto

Il fascicolo dell'iscritto riguarda tutta la gestione della documentazione relativa alla vita del medico, dell'odontoiatra e della società tra professionisti.

All'interno del titolo "Tenuta Albi" si distinguono tre voci di classificazione fondamentali per la tenuta degli Albi:

- Albo Medici chirurghi
- Albo Odontoiatri
- Albo Società tra professionisti

---

[8] La forma dell'Identificativo può essere stabilita dall'amministrazione che lo attribuisce. Un Identificativo deve essere compatibile con la formazione di un identificativo telematico come URI, cioè Uniform Resource Identifier (RFC 1738).

Regole aggiuntive:

- Un Identificativo è codificato mediante caratteri previsti dalla specifica US-ASCII a 8 bit ed è composto da una sequenza di lettere maiuscole ([A-Z]), lettere minuscole ([a-z]), cifre decimali ([0-9]) e dai caratteri '.', '-' e '_'.
- Un Identificativo deve avere una lunghezza non superiore a 16 caratteri.

Le prime due voci danno origine ad un fascicolo di persona fisica mentre nella terza si generano fascicoli di persona giuridica.

Ognuno di questi fascicoli è suddiviso in due differenti sottofascicoli:

- il sottofascicolo denominato DATI ISTITUZIONALI che comprende tutti i documenti relativi a titoli e requisiti necessari per l'effettiva iscrizione all'albo e per l'esercizio della professione
- il sottofascicolo denominato QUALIFICHE E ATTIVITA' che comprende tutti i documenti relativi all'attività professionale

Nel caso dei doppi iscritti deve essere aperto un fascicolo per ogni albo.

Nel caso in cui sia necessaria la gestione massiva di informazioni riferite a più iscritti (es. richiesta verifica autocertificazione del casellario giudiziario) viene generato un fascicolo unico annuale di attività da classificare nel titolo principale 3.0.

7.3.5 Dossier

Comprende tutti i documenti, anche con classifiche diverse e che possono appartenere a fascicoli o repertori differenti, che si riferiscono a una persona. Per spiegare meglio, nel DOSSIER personale di un iscritto all'Ordine o del personale dipendente ciascun documento viene classificato a seconda della classe di riferimento prevista e viene inserito nel fascicolo o nel repertorio di competenza.

Il dossier si configura così come aggregazione di documenti e si apre indipendentemente dalle classi del Titolario, perché riferito direttamente al soggetto sia esso ad una persona fisica o giuridica.

7.4 Repertori e fascicoli annuali

Il repertorio aggrega documentazione omogenea dal punto di vista formale, ma eterogenea sotto il profilo del contenuto giuridico e amministrativo: ad esempio verbali e deliberazioni di organi collegiali o monocratici, registrature contabili, ecc.

Si tratta di un peculiare tipo di aggregazione documentale che raccoglie documenti identici per forma e provenienza, ma difformi per contenuto, disposti in sequenza cronologica. Ciascun documento, in base a tale ordine, è identificato con un numero progressivo cui viene riconosciuta una valenza probatoria.

Il fascicolo annuale può raccogliere documentazione eterogenea sotto il profilo formale ma conservata insieme perché risultato di un medesimo processo di sedimentazione, o di una medesima attività, o perché relativa alla stessa materia.

Ai fini del loro facile reperimento, alcuni documenti, come i verbali, le deliberazioni degli organi di governo dell'Ente o i contratti, sono soggetti a registrazione di protocollo ed inseriti in un repertorio. I documenti possono essere altresì conservati in un fascicolo annuale, insieme ai documenti che afferiscono al medesimo argomento.

Sono repertoriate:

Convocazioni, Verbali e Delibere del Consiglio direttivo, della CAM e della CAO

Pagamenti elettronici (OIL)

7.5 Tipologie di registri

L'Ente gestisce altri registri esterni al protocollo, oltre a quello di protocollo informatico. Tali registri sono:

- Albo medici
- Albo odontoiatri
- Albo società tra professionisti
- Psicoterapeuti
- Medicine complementari
- Registro cronologico mandati
- Registro cronologico reversali
- Inventario beni mobili ed immobili

L'Ente ha in corso un processo di valutazione dei registri e delle dinamiche di gestione al fine di uniformare e centralizzare la gestione all'interno del software di gestione documentale e del protocollo informatico.

7.6 Organizzazione, gestione e strumenti dell'archivio unico corrente, di deposito e storico

Il sistema di protocollo informatico conserva nel suo archivio elettronico tutti i documenti originati e ricevuti ivi caricati dalla messa in esercizio dello stesso e pertanto funge da archivio corrente.

7.7 Piano di conservazione

Il piano di conservazione è uno strumento finalizzato a individuare le disposizioni di massima e definire i criteri e le procedure attraverso i quali i documenti e i fascicoli, non rivestendo interesse storico ai fini della conservazione permanente e avendo esaurito un interesse pratico e corrente, possono essere eliminati legalmente, previa autorizzazione della soprintendenza archivistica e bibliografica.

Le operazioni di selezione, necessarie a garantire la corretta gestione e la conservazione del complesso documentale dell'Ente, avvengono durante la fase di spostamento dall'archivio di deposito a quello storico, in modo tale da sedimentare solo la documentazione ritenuta rilevante ai fini della conservazione a lungo termine.

La proposta di scarto viene formulata secondo la procedura indicata dalla soprintendenza archivistica

Per i fascicoli informatici la proposta di scarto segue lo stesso iter per quanto riguarda l'autorizzazione della soprintendenza. Poiché l'Ordine affida ad un gestore esterno la conservazione dell'archivio di deposito e dell'archivio storico, il piano di conservazione verrà condiviso e adeguato ai protocolli richiesti.

7.7.1 Strumenti per la gestione dell'archivio di deposito

Periodicamente e secondo un apposito piano di versamento (di norma una volta all'anno), ogni singolo RPA (Responsabile del procedimento amministrativo) conferisce al RSP i fascicoli chiusi o comunque non più necessaria una trattazione corrente.

Questi fascicoli verranno trasmessi al conservatore in base al piano di conservazione predisposto.

7.7.2 Obbligo di conservazione, ordinamento e inventariazione dell'archivio storico

I documenti che costituiscono l'archivio storico sono conservati presso depositi dell'Ente e affidati alla gestione del Servizio archivistico. Essi devono essere ordinati e inventariati.

Anche se dichiarato bene culturale a tutti gli effetti dall'art. 10, comma 2, lettera b), del D.lgs 22 gennaio 2004, n. 42, Codice dei beni culturali e del paesaggio, l'organizzazione tecnico-scientifica dell'archivio storico, data la specificità del materiale, non può essere demandata alle strutture che si occupano di altri beni culturali (biblioteche, musei, etc.).

La consultazione dell'archivio storico è gestita direttamente dal Servizio archivistico.

8. PROCEDIMENTI AMMINISTRATIVI, ACCESSO AI DOCUMENTI E TUTELA DELLA RISERVATEZZA

8.1 Premessa

L'Ente, recependo le prescrizioni e i principi espressi dalla normativa in materia, ha disciplinato le attività e i procedimenti amministrativi definendo le responsabilità in ordine agli stessi.

In adempimento alla recente normativa in tema di trasparenza e accesso civico (Decreto legislativo n. 33 del 14 marzo 2013) l'Ente ha costituito apposita sezione di "Amministrazione trasparente" nel sito istituzionale, nella quale sono pubblicati dati, informazioni e documenti che riguardano l'organizzazione e le attività dell'amministrazione.

8.2 Procedure di accesso ai documenti e di tutela della riservatezza

Merita chiarire preliminarmente alcuni principi e procedure che costituiscono un punto di riferimento per chi opera presso l'Ente, tenendo conto che le problematiche connesse all'accesso e alla tutela della riservatezza riguardano tutte le fasi di vita dei documenti.

L'accesso/consultazione dei documenti si può così suddividere:

Consultazione per fini amministrativi, per la quale si fa riferimento allo specifico regolamento dell'Ente già citato, che può riguardare tutta la documentazione prodotta dall'Ente nell'esercizio della sua attività amministrativa, ivi compresa quella conservata nell'archivio storico.

Consultazione per fini di ricerca storico-scientifica, che è disciplinata dal Capo III del Codice dei Beni Culturali e del Paesaggio, in base al quale i documenti sono liberamente consultabili, ad eccezione:

- di quelli di carattere riservato relativi alla politica estera o interna dello Stato, che diventano consultabili 50 anni dopo la chiusura del fascicolo che li contiene;
- di quelli contenenti dati particolari, che diventano consultabili 40 anni dopo la chiusura del fascicolo che li contiene;
- di quelli contenenti taluni dati particolari idonei a rivelare lo stato di salute o la vita sessuale o i rapporti riservati di tipo familiare, che diventano consultabili 70 anni dopo la chiusura del fascicolo che li contiene.

La consultazione dei documenti contenenti dati particolari può essere autorizzata dalla Soprintendenza archivistica competente per territorio anche prima della scadenza dei termini prescritti dalla legge.

In ogni caso gli utenti che accedono alla documentazione conservata negli archivi storici sono tenuti al rispetto delle prescrizioni del Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi storici.

9. APPROVAZIONE E AGGIORNAMENTO DEL MANUALE, NORME TRANSITORIE E FINALI

9.1 Modalità di approvazione e aggiornamento del Manuale

Il presente Manuale è approvato dal Presidente con propria Determina Presidenziale n. 2 del 19/06/2025 e verrà aggiornato, su proposta del RSP o del gruppo di progetto incaricato della revisione, con le medesime modalità.

Gli aggiornamenti potranno rendersi necessari a seguito di:

- adeguamenti normativi che rendano superate le prassi definite nel Manuale
- introduzione di nuove pratiche tendenti a migliorare l'azione amministrativa in termini di efficacia, efficienza e trasparenza
- inadeguatezza delle procedure rilevate nello svolgimento delle attività correnti

Gli allegati al presente Manuale contengono indicazioni di dettaglio sulle procedure operative e sulle modalità di funzionamento dei sistemi gestionali.

Il Manuale entra in vigore alla data di esecutività della Determina che lo approva.

9.2 Pubblicità del presente Manuale

In ottemperanza a quanto disposto dal comma 3 dell'art. 5 del DPCM 3 dicembre 2013, il Manuale di gestione è reso pubblico dall'Ordine mediante la pubblicazione sul proprio sito istituzionale https://www.ordinedeimedici.cb.it/trasparenza-2/

Al fine di assicurarne adeguata conoscenza al personale dell'Ente l'utilizzo del Manuale di gestione viene inserito nei percorsi di formazione del personale in tema di gestione documentale.

Allegato 1 - Glossario dei termini e degli acronimi

TERMINE	DEFINIZIONE
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
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
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 organizzativa omogenea – AOO	un 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 (D.P.C.M. 3 dicembre 2013, allegato 1)
Autenticità	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 di dati	collezione di dati registrati e correlati tra loro
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 metadati
Certificati elettronici	gli attestati elettronici che collegano all'identità del titolare i dati utilizzati per verificare le firme elettroniche
Certificatore accreditato	soggetto, pubblico o privato, che svolge attività di certificazione del processo di conservazione al quale sia stato riconosciuto, dall' Agenzia per l'Italia digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza
Codice dell'amministrazione digitale	decreto legislativo 7 marzo 2005, n. 82. Testo di riferimento per le pubbliche amministrazioni sulla gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale
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 e descritto nel manuale di conservazione
Cooperazione applicativa	la parte del sistema pubblico di connettività finalizzata all'interazione tra i sistemi informatici delle pubbliche amministrazioni per garantire l'integrazione dei metadati, delle informazioni e dei procedimenti amministrativi
Copia informatica di documento analogico	il documento informatico avente contenuto identico a quello del documento analogico da cui è tratto
Copia informatica di documento informatico	il documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari
Copia per immagine su supporto informatico di documento analogico	il documento informatico contenuto e forma identici a quelli del documento analogico da cui è tratto
Documento informatico	la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
Documento analogico	la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti
Domicilio digitale del cittadino	indirizzo PEC popolazione residente – ANPR per la trasmissione in via telematica informazioni o dati
Duplicato informatico	il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario

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 dell'Amministrazione digitale
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
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
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
Formato	modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico comunemente è identificato attraverso l'estensione del file
Gestione dei documenti	l'insieme delle attività finalizzate alla registrazione e segnatura di protocollo, nonché alla classificazione, organizzazione, assegnazione, reperimento e conservazione dei documenti amministrativi formati o acquisiti dalle amministrazioni nell'àmbito del sistema di classificazione d'archivio adottato, effettuate mediante sistemi informatici
Identificazione informatica	la validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne consentono l'individuazione nei sistemi informativi, effettuata attraverso opportune tecnologie anche al fine di garantire la sicurezza dell'accesso
Identificativo univoco	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
Immodificabilità	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
Interoperabilità	possibilità di trattamento automatico, da parte di un sistema di protocollo ricevente, delle informazioni trasmesse da un sistema di protocollo mittente, allo scopo di automatizzare anche le attività ed i processi amministrativi conseguenti (articolo 55, comma 4, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e articolo 17 del Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013)
Log di sistema	registrazione cronologica delle operazioni eseguite su di un sistema informatico per finalità di controllo e verifica degli accessi, oppure di registro e tracciatura dei cambiamenti che le transazioni introducono in una base di dati
Manuale di gestione	strumento che descrive il sistema di gestione informatica dei documenti di cui all'articolo 5 delle regole tecniche del protocollo informatico D.P.C.M. 3 dicembre 2013
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
Piano della sicurezza del sistema di gestione informatica dei documenti	documento, che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di gestione informatica dei documenti da possibili rischi nell'ambito dell'organizzazione di appartenenza
Piano di conservazione	strumento, integrato con il sistema di classificazione per la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'articolo 68 del D.P.R. 28 dicembre 2000, n. 445
Piano generale della sicurezza	documento per la pianificazione delle attività volte alla realizzazione del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio nell'ambito dell'organizzazione di appartenenza
Posta elettronica certificata	sistema di comunicazione in grado di attestare l'invio e l'avvenuta consegna di un messaggio di posta elettronica e di fornire ricevute opponibili ai terzi

Portale	sito Internet che indirizza l'utente verso il reperimento di informazioni e servizi all'interno del sito stesso o in generale sul web
Registro particolare	registro informatico di particolari tipologie di atti o documenti nell'ambito della pubblica amministrazione è previsto ai sensi dell'articolo 53, comma 5 del D.P.R. 28 dicembre 2000, n. 445
Registro di protocollo	registro informatico di atti e documenti in ingresso e in uscita che permette la registrazione e l'identificazione univoca del documento informatico all'atto della sua immissione cronologica nel sistema digestione informatica dei documenti
Repertorio informatico	registro informatico che raccoglie i dati registrati direttamente dalle procedure informatiche con cui si formano altri atti e documenti o indici di atti e documenti secondo un criterio che garantisce l'identificazione univoca del dato all'atto della sua immissione cronologica
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'art. 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 del trattamento dei dati	la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali
Responsabile della sicurezza	soggetto al quale compete la definizione delle soluzioni tecniche ed organizzative in attuazione delle disposizioni in materia di sicurezza
Scarto	operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e 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
Segnatura di protocollo	l'apposizione o l'associazione, all'originale del documento, in forma permanente e non modificabile delle informazioni riguardanti il documento stesso.
Sistema di conservazione	sistema di conservazione dei documenti informatici di cui all'art. 44 del Codice dell'amministrazione digitale
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
Trasmissione telematica	trasmissione di documenti attraverso servizi di telecomunicazione
Utente	persona, 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
Unità organizzativa responsabile – UOR	un ufficio della AOO che utilizza i servizi messi a disposizione dal sistema di protocollo informatico (D.P.C.M. 3 dicembre 2013, allegato 1).
Validazione temporale	il risultato della procedura informatica con cui si attribuiscono, aduno o più documenti informatici, una data ed un orario opponibili ai terzi.

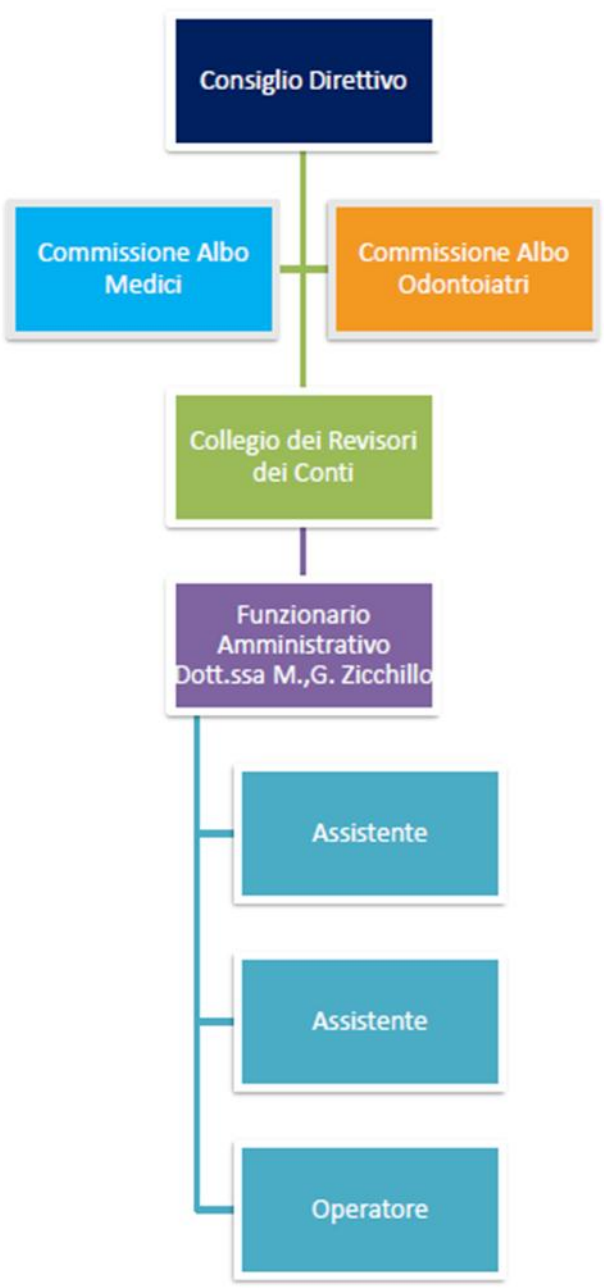
Allegato 2 - Individuazione AOO

Ordine dei Medici Chirurghi e degli Odontoiatri della Provincia di Campobasso

codice IPA: **odmcd_cb**

Codice Univoco AOO	Denominazione AOO	Domicilio Digitale	Indirizzo	Ulteriori Informazioni
A735DA6	Ordine Medici Campobasso	Dal 12/04/2019 ad oggi: info.cb@pec.omceo.it	Via Mazzini, 129/A - Campobasso (CB)	AOO

Allegato 3 – Organigramma



Allegato 4 - Istituzione del "Servizio archivistico dell'Ordine" e individuazione del Responsabile del Servizio

DELIBERAZIONE CD N. 64 DEL 09/06/2025

Allegato 5 – Titolario

Indice	ID	Classe
00	1000	Gestioni speciali
00.01	1001	Documenti classificati prima del presente Titolario
01	**1002**	**Amministrazione generale**
01.01	1003	Legislazione, comunicazioni e circolari esplicative, Legge istitutiva e regolamento attuativo
01.02	1004	Piani, regolamenti e modulistica
01.03	1005	Politica del personale, ordinamento degli uffici e dei servizi
01.04	1006	Controlli interni ed esterni
01.05	1007	Cerimoniale, attività di rappresentanza, onorificenze e riconoscimenti
01.06	1008	Assicurazioni
01.07	1009	Progetti di sviluppo e organizzazione in fase di progettazione
01.08	1010	Certificazione di Qualità (ISO)
01.09	1011	Accesso agli atti, Accesso civico semplice e generalizzato
01.10	1012	Organizzazione e accreditamento eventi ECM
01.11	1113	Accreditamento e Richiesta sala dell'Ordine
01.12	1129	Convenzioni, accordi, protocolli di intesa
02	**1013**	**Organi di governo**
02.01	1014	Consiglio e cariche istituzionali
02.02	1015	Collegio Revisori dei Conti
02.03	1016	Commissione Albo Medici Chirurghi
02.04	1017	Commissione Albo Odontoiatri
02.05	1018	Commissione Pari Opportunità
02.06	1019	Commissione per le medicine complementari
02.07	1020	Gruppi di lavoro e altre commissioni
02.08	1021	Rappresentanza politica dell'Ordine presso Enti, Istituzioni e assimilati
02.09	1022	Elezione organi istituzionali
02.10	1023	Arbitrati, Nomine e Designazioni
02.11	1024	Assemblee ordinaria straordinaria ed elettorale
02.12	1114	Federazioni Regionali degli Ordini dei Medici Chirurghi e degli Odontoiatri
02.13	1115	Osservatori, indagini, studi e pubblicazioni
03	**1025**	**Tenuta Albi**
03.01	1026	Albo medici Chirurghi e Albo Odontoiatri
03.02	1027	Albo Società tra Professionisti
03.03	1028	Qualifiche professionali
03.04	1029	Albo CTU e CTP
03.05	1030	Medici Competenti
03.06	1031	Prestazioni di servizio Medici e Odontoiatri stranieri

03.07	1032	Medici Psicoterapeuti
03.08	1033	Medicine complementari
03.09	1034	Aggiornamento professionale ed ECM
03.10	1035	Rilascio credenziali di accesso (PIN)
03.11	1036	Certificati, attestazioni, autocertificazioni
03.12	1037	Denuncia furti e smarrimenti
03.13	1038	Comunicazioni relative alla tenuta degli albi
03.14	1039	Professione medica e odontoiatrica (circolari, regolamenti e norme)
03.15	1040	Segnalazioni, Convocazioni e Audizioni
03.16	1041	Procedimenti disciplinare agli iscritti
03.17	1042	Richiesta PEC e comunicazioni
03.18	1043	Richieste informazioni su tenuta Albi
03.19	1116	Albo Medici Chirurghi
03.20	1117	Albo Odontoiatri
03.21	1118	Segnalazioni e Procedimenti disciplinari
03.22	1119	Flussi documentali FNOMCeO ed ENPAM
04	**1044**	**Tutela della professione e rapporti con gli Iscritti**
04.01	1045	Quesiti e istanze
04.02	1046	Comunicati Stampa
04.03	1047	Pubblicità dell'informazione sanitaria
04.04	1048	Pareri di congruità parcelle e tariffario
04.05	1049	Autorizzazioni e accreditamento per l'attività professionale
04.06	1120	Tutoraggi, tirocini e stage
04.07	1121	Borse di studio e corsi MMG
04.08	1122	Servizi per gli iscritti
04.09	1123	Segnalazioni non riferite al singolo iscritto
05	**1050**	**Comunicazione, sistemi informativi**
05.01	1051	Servizi vari per gli iscritti
05.02	1052	Congressi e manifestazioni
05.03	1053	Patrocini
05.04	1054	Segnalazioni non riferite al singolo iscritto
05.05	1055	Accreditamento e Richiesta sala dell'Ordine
05.06	1056	Comunicazione, informazione
05.07	1057	Tutoraggi, tirocini e stage
05.08	1058	Borse di studio e corsi MMG
05.09	1124	Comunicati Stampa
05.10	1125	Sistemi informatici
06	**1059**	**Risorse umane**

06.01	1060	Concorsi Selezioni e colloqui
06.02	1061	Collaborazioni esterne e Stage
06.03	1062	Assunzioni e cessazioni – Mobilità; Comandi e distacchi
06.04	1063	Attribuzioni di funzioni, ordini di servizio
06.05	1064	Inquadramenti e applicazioni contratti collettivi di lavoro
06.06	1065	Retribuzioni, compensi, accessori, TFR
06.07	1066	Tutela della salute e sicurezza sul luogo di lavoro
06.08	1067	Contenzioso
06.09	1068	Presenze, assenze e orari di lavoro
06.10	1069	Giudizi, responsabilità e provvedimenti disciplinari
06.11	1070	Formazione e aggiornamento professionale
06.12	1126	Trattamento (posizione) giuridico ed economico del dipendente
06.13	1127	Giudizi, responsabilità e provvedimenti disciplinari e contenzioso
07	**1071**	**Risorse Finanziarie, Patrimoniali e strumentali**
07.01	1072	Bilanci, Variazioni di Bilancio, Rendiconti.
07.02	1073	Contratti, Incarichi e Collaborazioni professionali
07.03	1074	Procedure negoziate, bandi e gare
07.04	1075	Fatture PA (e note di credito)
07.05	1076	Notifiche SDI
07.06	1077	Gestione delle entrate e riscossioni
07.07	1078	Reversali
07.08	1079	Gestione delle uscite
07.09	1080	Mandati
07.10	1081	O.I.L. Ordinativi Elettronici Tesoreria
07.11	1082	Gettoni di presenza
07.12	1083	DDT e Rapporti di intervento
07.13	1084	Adempimenti fiscali, contributivi e assicurativi
07.14	1085	Beni Mobili e Immobili (compresi accessori informatici)
07.15	1086	Mutui
08	**1087**	**Previdenza**
08.01	1088	Gestione ENPAM
08.02	1089	Commissione Invalidità ENPAM
08.03	1090	Varie altri enti previdenziali e assistenziali
09	**1091**	**Relazioni istituzionali con altri Enti ed Associazioni**
09.01	1092	FNOMCeO
09.02	1093	REGIONE
09.03	1094	Federazioni Regionali degli Ordini dei Medici Chirurghi e degli Odontoiatri
09.04	1095	Altri ordini e Collegi professionali Medici e non medici

09.05	1096	Relazioni istituzionali con soggetti di diritto pubblico
09.06	1097	Relazioni istituzionali con soggetti di diritto privato
09.07	1098	Associazioni Sindacali – Culturali Mediche
09.08	1099	Aggregazioni territoriali Mediche (UTAP – medicine di gruppo)
09.09	1100	Associazioni di Volontariato
09.10	1101	Elezioni e nomine altri enti
09.11	1102	Osservatori, indagini, studi e pubblicazioni
10	**1103**	**Risorse documentali**
10.01	1104	Registro giornaliero di protocollo
10.02	1105	Rapporti di versamento
10.03	1106	Scarti
10.04	1128	Gestione dell'archivio
11	**1107**	**Affari Legali**
11.01	1108	Contenzioso
11.02	1109	Pareri e consulenze
11.03	1110	Arbitrati
12	1111	Oggetti diversi
12.01	1112	Oggetti diversi

Allegato 6 – Oggettario

Accreditamento evento residenziale n.
Accusa ricevuta fascicolo personale
ACN Medici di Medicina Generale
ACN Pediatri di Libera Scelta: comunicazione pubblicazione zona carente straordinaria
ACN Specialisti Ambulatoriali Interni
Adempimenti relativi alla trasparenza amministrativa - richiesta documenti
Aggiornamento tabelle contenenti indicazioni sostanze stupefacenti e psicotrope
Assegnazione credenziali di accesso al Sistema TS
Attestato di manutenzione dell'impianto elettrico
Attestato partecipazione corso perfezionamento
Attestato per riconoscimento crediti ECM
Attestazione iscrizione all'ordine per pratica adozione
Attestazione periodo di maternità per registrazione esonero ECM
atto di accertamento inosservanza obbligo vaccinale dott./d.ssa
Atto di citazione avanti il Giudice di Pace
Atto di nomina a legale di fiducia e procura speciale
Autocertificazione corso di perfezionamento
Autocertificazione diploma triennale in Medicina Generale
Autocertificazione Master Universitario I livello in …
Autocertificazione Master Universitario II livello in …
Autocertificazione regolarità contributiva
Autocertificazione regolarità contributiva e copia documento di identità legale rappresentante
Autocertificazione riconoscimento Ministero della specializzazione in ….
Autocertificazione specializzazione in …
Autocertificazione variazione indirizzo di residenza
Avviso di pagamento Contributo di bonifica
Avviso di pagamento Contributo di bonifica
Avviso di pagamento servizio rifiuti TARSU
Avviso pubblicazione incarichi vacanti Continuità assistenziale
Avviso pubblicazione zone carenti assistenza primaria
Avviso pubblico per conferimento incarichi assistenza sanitaria notturna ai turisti
Avviso scadenza polizza antincendio sede Ordine
Bando di concorso per ammissione corso triennale di formazione specifica in medicina generale triennio ..
Bando di concorso per l'ammissione al corso triennale di formazione specifica in medicina generale: trasmissione avviso convocazione dei candidati ammessi
Bilancio Consuntivo anno .....
Bilancio Preventivo anno .....
Centri Regionali autorizzati a prescrizione farmaci: invio decreti

Certificato Carichi Pendenti
Certificato Casellario Giudiziale
Certificato di Good Standing per paesi extra CEE
Certificato di Iscrizione all'Ordine
Certificato di morte .....
Certificato differimento vaccino
Certificato esenzione vaccino
Certificazione Unica - CU
Cessazione per dimissioni incarico di ….
Cessazione rapporto convenzionale
Circolare Ministero delle Finanze
Codice Deontologico
Comunicato stampa
Comunicazione accettazione offerta
Comunicazione accettazione preventivo
Comunicazione adesione a bando
Comunicazione ai sensi dell'art. 38 comma 3 Dlgs. 81/2008 e dell'art. 2 comma 2 D.M. Lavoro 4.3.2009: conseguimento crediti formativi
Comunicazione AIFA
Comunicazione annullamento iscrizione
Comunicazione apertura e sospensione procedimento disciplinare
Comunicazione archiviazione procedimento disciplinare
Comunicazione assegnazione CIG
Comunicazione assunzione incarico direttore sanitario
Comunicazione avviso pubblico
Comunicazione cambio Direttore Responsabile del Notiziario
Comunicazione cancellazione Albo Medici Chirurghi per
comunicazione cancellazione Albo Odontoiatri per
Comunicazione cancellazione dall'albo per morosità ed irreperibilità
Comunicazione cancellazione ed invio fascicolo personale
Comunicazione chiusura/spostamento studio
Comunicazione costituzione Medicina di Gruppo
Comunicazione costituzione UTAP
Comunicazione decesso .....
Comunicazione decisione disciplinare
Comunicazione di nuovo IBAN per addebito quota
Comunicazione dimissioni .....
Comunicazione disattivazione PEC
Comunicazione erogazione contributo

Comunicazione esito esame dei preventivi
Comunicazione Fnomceo n. .....
Comunicazione furto timbro e ricettari azienda ulss
Comunicazione indirizzo PEC
Comunicazione iscrizione Albo Medici Chirurghi
Comunicazione iscrizione Albo Medici Chirurghi e Albo Odontoiatri
Comunicazione iscrizione Albo Odontoiatri
Comunicazione iscrizione albo periti e consulenti tecnici del tribunale_pagamento Tassa Concessione governativa
Comunicazione iscrizione Albo Società tra Professionisti - STP
Comunicazione non partecipazione del presidente
Comunicazione opzione regime di impegno a tempo pieno dal ..
Comunicazione prestazione di servizio anno ..
Comunicazione radiazione dall'esercizio professionale
Comunicazione reiscrizione all'albo con soluzione di continuità
Comunicazione sospensione dall'esercizio professionale
Comunicazione variazione nome e codice fiscale
Concessione patrocinio .....
Conferimento incarico .....
Conferimento incarico temporaneo continuità assistenziale
Conferimento incarico temporaneo MMG
Conferimento incarico temporaneo per sostituzione ex art. 34 ACN Medici specialisti ambulatoriali
Conferimento incarico temporaneo specialistica ambulatoriale
Conferma autocertificazione iscrizione
Conferma dati autocertificati da .....
Conferma dati per trasferimento
Conferma Esame di Stato .....
Conferma Laurea .....
Conferma Laurea ed Esame di Stato
Conferma prenotazione stanze
Contrattazione decentrata
Contratto apertura conto deposito
Contratto di collaborazione
Contributo straordinario
Convenzione Banca S. Stefano/OMCeO VE
Convocazione ai sensi dell'art. 11 DLgs 233/46
Convocazione Assemblea CAO Nazionale
Convocazione Assemblea Enpam
Convocazione Assemblea Ordinaria degli Iscritti

Convocazione Assemblee Elettorali
Convocazione Celebrazione Disciplinare
Convocazione Collegio Revisori dei Conti
Convocazione Comitato Federativo Fromceo Veneto
Convocazione Commissione Albo Medici Chirurghi
Convocazione Commissione Albo Odontoiatri
Convocazione Commissione Invalidità
Convocazione Consiglio Direttivo
Convocazione Consiglio Federazione Regionale Ordini del Veneto
Convocazione Consiglio Nazionale Fnomceo
Convocazione coordinamento segreterie del Veneto
Convocazione ex art. 39 DPR 221/50
Convocazione OOSS per Contrattazione decentrata Omceo Venezia
Convocazione per apertura buste per assegnazione servizio ..
Convocazione per comunicazioni in merito a …..
Convocazione riunione Comitato esaminatore richieste iscrizione CTU e Albo Periti
Copia conforme all'originale
Copia denuncia smarrimento tesserino di iscrizione dell'ordine
Copia sentenza tribunale …….
Corsi di aggiornamento personale
Corso Triennale Formazione Specifica in MG: ammissione ed esclusione concorrenti
Corso Triennale Formazione specifica in MG: costituzione commissione colloquio finale e rilascio diplomi
Corso Triennale Formazione specifica in MG: nominativi per commissione colloquio finale e rilascio diplomi
Curriculum vitae per cinquantesimo di laurea
Curriculum Vitae per collaborazione personale di segreteria
Debito formativo ECM: autocertificazione stato pensionamento
Delega alla gestione della posizione contributiva, invio denunce mensili, gestione adempimenti nei confronti di terzi mediante denunce medesime
Delega gestione posizione contributiva committente/associante Omceo Ve, invio denunce mensili, gestione adempimenti nei confronti di terzi mediante denunce medesime, con rif. a collaboratori
Delega per tenuta del libro unico del lavoro
Delibera CAM …….
Delibera n……
Delibera n° .... dott XY : annotazione della sospensione ex DL 172/2021
Denuncia dichiarazioni mendaci
Dichiarazione di impegno ad effettuare la presentazione telematica del modello DASM - denuncia mensile INPGI
Dichiarazione di insussistenza di cause di inconferibilità e incompatibilità di incarichi c/o P.A. ai sensi del D.Lgs.39/2013 ANNO ….
Dichiarazione sostitutiva possesso requisiti generali e di capacità economico-finanziaria e tecnica
Dichiarazione sottoscritta per ritiro chiavi e deposito cauzionale uso sala ordine

Diffida per mancata comunicazione domicilio digitale_PEC
Documentazione integrativa per .....
Documentazione per inserimento esonero ECM
Documento Regolarità Contributiva - DURC
Documento unico di Valutazione dei Rischi - DVR
Domanda ammissione concorso Area Funzionale "B" - posizione economica"B1" - a tempo indeterminato – profilo professionale di Operatore amministrativo
Domanda di cancellazione dall'Albo Medici Chirurghi
Domanda di cancellazione dall'Albo Medici Chirurghi e dall'Albo Odontoiatri
Domanda di cancellazione dall'Albo Odontoiatri
Domanda di inserimento elenco per Commissione esame finale corso ASO
Domanda di iscrizione all'elenco degli Psicoterapeuti
Domanda di iscrizione all'elenco Esercenti le Medicine Complementari
Domanda iscrizione Albo Medici Chirurghi per trasferimento da
Domanda iscrizione Albo Odontoiatri per trasferimento da
Domanda iscrizione Albo Società tra Professionisti - STP
Domanda prima iscrizione Albo Medici Chirurghi
Domanda prima iscrizione Albo Odontoiatri
Dott XY : comunicazione annotazione della sospensione ex DL 172/2021
ECM Piano formativo Fnomceo: richiesta programmi formativi per aderenti paternariato
Elenchi nominativi con crediti ECM del corso FAD
Erogazione prima mensilità pensione enpam
Esame di Stato per l'abilitazione all'esercizio della professione di medico chirurgo: Reclutamento Tutori
Esito verifica regolarità contributiva
Giornata del Medico
Impugnazione sanzione disciplinare
Individuazione dei Centri Regionali autorizzati alla prescrizione di farmaci: inoltro decreti
Invio Albi professionali ai sensi dell'art. 2 DPR 221/50
Invio Albi professionali ai sensi dell'art. 2 DPR 221/50
Invio Decisioni Comitato Centrale del
Invio estremi pagamento quota causa fallito addebito
Invito a convegno .....
Iscrizione provvisoria negli elenchi di pediatria di libera scelta per la copertura della zona carente del distretto …
Istanza di accesso agli atti
Istanza di ammissione per la formazione di elenchi di imprese da invitare alle procedure ristrette semplificate
Istanza di candidatura alle procedure ad invito diretto
Lettera di incarico per .....
Memoria sui fatti oggetto della convocazione ex art. 39
Modello SDD per addebito quota ordine
Nomina a difensore di fiducia in merito al procedimento penale

Nomina Amministratore di sistema
Non accettazione offerta per .....
Non accettazione preventivo
Non concessione patrocinio
Notifica esito elezioni triennio .....
Notifica graduatoria regionale definitiva anno
Notifica graduatoria regionale provvisoria anno
Offerta per la fornitura .....
OIL Ordinativo Elettronico di pagamento / incasso
Ordinativo buoni pasto personale dipendente mesi
Osservatorio regionale per gli studi di settore: richiesta nomina referente
Parere di congruità parcella
Parere per pubblicità sanitaria
Permesso di soggiorno
Prenotazione seconda dose vaccino
Prenotazione servizio asporto rifiuti ingombranti
Prenotazione terza dose vaccino
Preventivo .....
Proroga contratto
Protocollo d'intesa
Quesiti
Rapportini lavoro agile e verbali riunioni segreteria mese ....
Rapporto di Versamento Registro di Protocollo
Rendicontazione spese
Ricevuta Agenzia delle Entrate acquisizione file ExpAnagTribu anno ..
Ricevuta pagamento quota ordine anno
Richiesta accreditamento per utilizzo sala ordine
Richiesta apertura partita IVA
Richiesta appuntamento
Richiesta attestato assolvimento crediti ECM triennio .....
Richiesta attestato iscrizione all'ordine per pratica adozione
Richiesta atti convegno
Richiesta attivazione Casella Posta Elettronica Certificata
Richiesta attivazione SPID con documenti
Richiesta Certificato Carichi Pendenti
Richiesta Certificato Casellario Giudiziale
Richiesta certificato di iscrizione all'Ordine
Richiesta conferma autocertificazione conseguimento Corso di Perfezionamento

Richiesta conferma autocertificazione conseguimento diploma triennale in Medicina Generale
Richiesta conferma autocertificazione conseguimento Master ..
Richiesta conferma autocertificazione specializzazione in ….
Richiesta conferma dati per trasferimento
Richiesta conferma dichiarazioni sostitutive iscrizione all'albo
Richiesta conferma Laurea ed Esame di Stato
Richiesta copia fascicolo disciplinare
Richiesta copia verbale audizione
Richiesta credenziali di accesso al Sistema TS
Richiesta curriculum vitae
Richiesta duplicato tesserino ordine
Richiesta elenco medici competenti del lavoro
Richiesta esito procedimento disciplinare
Richiesta informazioni
Richiesta inserimento in elenco medici disponibili per le sostituzioni
Richiesta integrazione quota iscrizione anno ….. ai sensi della delibera n.10/2015
Richiesta parere congruità parcella
Richiesta parere pubblicità sanitaria
Richiesta patrocinio
Richiesta permesso di soggiorno
Richiesta permesso retribuito ex art. 25 del CCNL per motivi personali
Richiesta permesso retribuito ex art. 26 del CCNL per visite, terapie, prestazioni specialistiche o esami diagnostici
Richiesta pubblicazione annuncio
Richiesta riconoscimento professionalità acquisita in ..
Richiesta rilascio permessi ZTL
Richiesta rimborso
Richiesta rinnovo permessi ZTL
Richiesta utilizzo sala
Ricorso avanti CCEPS avverso decisione disciplinare
Rilevazione censuaria delle istituzioni pubbliche
Rilevazione del fabbisogno delle professioni sanitarie e del fabbisogno di laureati magistrali delle professioni sanitarie anno …
Rinnovo cariche
Risposta a quesito
Risposta a richiesta parere
Segnalazione
Segnalazione anonima
Sentenza Corte Cassazione Civile n. ...
Sentenza TAR Lazio n. .....

Sollecito invio documentazione
Sollecito invio memoria
Sollecito pagamento diritti per parere congruità parcella del
Sospensione cautelare dall'esercizio professionale
Sospensione esercizio professionale
Sospensione ope legis ex art. 43 DPR 221/1940
Trasmissione domanda di pensione anticipata quota A
Trasmissione Albi professionali ai sensi dell'art. 2 DPR 221/50
Trasmissione atti per ricorso n. .....
Trasmissione delega per Assemblea Nazionale Enpam
Trasmissione delega per Consiglio Nazionale Fnomceo
Trasmissione delibera ai sensi art. 35 dpr 221 per approvazione Fnomceo
Trasmissione delibera decorrenza periodo di sospensione
Trasmissione documentazione per richiesta esonero vaccinazione sars Covid 19 dott./d.ssa ...
Trasmissione domanda di indennità per inabilità temporanea
Trasmissione domanda di pensione di vecchiaia Quota A
Trasmissione domanda di pensione Fondi Speciali
Trasmissione domanda di prestazione assistenziale una tantum
Trasmissione domanda di sussidio continuativo per assistenza domiciliare Enpam
Trasmissione domanda pensione di reversibilità
Trasmissione domanda sussidio per calamità naturali
Trasmissione file dati anagrafici/ professionali del .... a mezzo applicativo
Trasmissione modulo per esercizio diritto di opzione per calcolo pensione anticipata 65° anno
Trasmissione Note Aifa relative a
Trasmissione richieste permessi ZTL
Trasmissione sanzione disciplinare aziendale a carico di ...
Variazioni al bilancio preventivo anno …
Verbale Assemblea Ordinaria del .....
Verbale audizione ex art. 39
Verbale audizione per comunicazioni
Verbale CAO Nazionale del .....
Verbale Comitato Federativo del .....
Verbale Commissione Albo Medici Chirurghi del ..
Verbale Commissione Albo Odontoiatri del .....
Verbale Commissione Pari Opportunità del ..
Verbale Consiglio Direttivo del .....
Verbale Consiglio Nazionale Fnomceo del ..
Verbale denuncia furto

Verbale Gruppo di Lavoro Comunicazione Sito e Notiziario
Verbale Gruppo Giovani medici del

Allegato 7 – Piano di fascicolazione

CLASSE DEL TITOLARIO	DENOMINAZIONE DEL FASCICOLO	TIPOLOGIA DEL FASCICOLO	DESCRIZIONE DEL FASCICOLO	DURATA DEL FASCICOLO
01 Amministrazione generale			**Questo titolo è stato pensato per tutti i documenti prodotti a vario livello nell'esercizio di funzioni di carattere generale e trasversale dell'Ente. Tali documenti interessano tutti gli uffici in quanto costituiscono strumento interpretativo e di indirizzo per l'attività amministrativa dell'Ordine. Nel contempo vengono inseriti in questo titolo le classi documentali riferite le attività di amministrazione dell'Ente e gli adempimenti relativi alla trasparenza amministrativa e all'accesso agli atti.**	
Legislazione, comunicazioni e circolari esplicative, Legge istitutiva e regolamento attuativo	**Comunicazioni FNOMCeO e OMCeO italiani**	Affare o attività	Devono essere inserite in questa classe tutte le circolari interpretative e di approfondimento delle norme sull'amministrazione generale dell'ente, oltre all'attività interpretativa e di modifica/integrazione delle leggi e regolamenti che disciplinano l'organizzazione dell'ente	fascicolo annuale
	Legge di riforma degli Ordini 03/2018	Affare o attività	documentazione relativa alla legge di riforma degli ordini (circolari, regolamenti attuativi etc) di qualsiasi provenienza	fascicolo annuale
	Comunicazioni da parte di altri ENTI	Affare o attività	Comunicazioni da parte di Enti diversi da FNOMCeO (ANAC, AGENAS, MINISTERI, COGEAPS etc) relative alla gestione dell'Ordine e agli adempimenti di competenza ordinistica.	fascicolo annuale
Piani, regolamenti e modulistica	**Nome Regolamento**	Procedimento amministrativo	fascicolo dedicato al procedimento in oggetto, contiene tutti i documenti relativi alla stesura, approvazione e trasmissione a fnomceo per l'approvazione in CC – compresa eventuale modulista (es accesso	fascicolo per regolamento, si chiude con l'approvazione del regolamento da parte del CC Fnomceo (dopo aver atteso la scadenza dei termini di silenzio-assenso da parte del Ministero della Salute)
	Nome Piano	Affare o attività	fascicolo dedicato al procedimento in oggetto, contiene tutti i documenti relativi alla stesura, approvazione ed eventuale pubblicazione – compresa eventuale modulistica specifica per piano (es DVR, piano anticorruzione)	fascicolo per piano
	Modulistica	Affare o attività	documenti relativi ad altri moduli approvati e resi disponibili dall'Ordine non legati a specifici regolamenti e piani	fascicolo annuale
Politica del personale, ordinamento degli uffici e dei servizi	**Comunicazioni su gestione del personale**	Affare o attività	circolari e comunicazioni FNOMCeO,altri enti e dal Consulente del lavoro relative alla applicazione del CCNL e norme correlate e destinate	fascicolo annuale
	Piano triennale del fabbisogno del personale	Affare o attività	Documenti relativi redazione e approvazione del piano	fascicolo per piano, si chiude con approvazione del CC fonmceo (dopo aver atteso la scadenza dei termini di silenzio-assenso da parte del Ministero della Salute)
Controlli interni ed esterni		Affare o attività	comunicazioni anagrafe tributaria, perla pa, istat, etc	fascicolo annuale
	Controlli e adempimenti interni	Affare o attività	segnalazioni e comunicazioni pervenute per es. da Collegio dai revisori dei conti, DPO, RPCT, RSSL ecc.	fascicolo annuale
Cerimoniale, attività di rappresentanza, onorificenze e riconoscimenti	**Giornata del Medico**	Affare o attività	documentazione relativa all'organizzazione e gestione della giornata del medico: inviti, comunicazioni etc	fascicolo per evento
	Celebrazioni correlate alla Professione	Affare o attività	Varie manifestazioni quali, l'accoglienza dei neo iscritti, ecc.	fascicolo per evento
	rappresentanza/onoreficenze	Affare o attività	comunicazioni di congratulazioni, ringraziamenti etc	fascicolo annuale
Progetti di sviluppo e organizzazione	**Fascicolo per progetto**	Affare o attività	documenti relativi a progetti, tavoli di lavoro etc che riguardano l'attività dell'ente (es. alternanza scuola-lavoro)	fascicolo per progetto
Certificazione di Qualità (ISO)	**Certificazione di qualità ISO *****	Procedimento amministrativo	documentazione relativa alle pratiche per ottenere la certificazione ISO e alle verifiche periodiche da parte dell'Autority certificante	fascicolo per procedimento
			documentazione relativa alle istanze di	fascicolo per procedimento: si apre con istanza di accesso e si chiude con

Accesso agli atti, Accesso civico semplice e generalizzato	**fascicolo per istanza specificando tipologia di accesso**	Procedimento amministrativo	accesso agli atti ex L 241/90	dichiarazione di presa visione degli atti richiesti.
			documentazione relativa alle istanze di accesso civico	fascicolo per procedimento: si apre con richiesta di immediata pubblicazione e si chiude con dichiarazione di avvenuta pubblicazione degli atti richiesti.
			documentazione relativa alle istanze di accesso generalizzato	fascicolo per procedimento: si apre con istanza di accesso e si chiude con dichiarazione di presa visione degli atti richiesti.
Organizzazione e accreditamento eventi ECM	**Fascicolo con Nome evento**	Affare o attività	documentazione relativa all'accreditamento, invito ai relatori, richieste patrocini a terzi, slides etc (le procedure per affitto sala e catering rientrano in "procedure negoziate, bandi e gare")	fascicolo per evento, si apre con la richiesta di accreditamento e si chiude con la conferma di inserimento del report nel portale AGENAS o trasmissione documentazione e report di fine evento alla FNOMCeO in caso di partenariato.
Accreditamento e Richiesta sala dell'Ordine	**Richieste uso sala convegni/riunioni**	Affare o attività	documentazione relativa a richieste e concessioni della sala convegni/riunioni a iscritti, associazioni etc.	fascicolo annuale/fascicolo per richiesta (a seconda della complessità)
Convenzioni, accordi, protocolli di intesa	**Fascicolo con denominazione dell'attività e del soggetto corrispondente**	Affare o attività	accordi per accesso a banche dati università, protocolli di intesa, convenzioni FNOMCEO per servizi agli ordini (PEC, ebsco)	fascicolo per attività

2 Organi di governo			**Questo titolo è stato pensato per gli atti concernenti gli organi di governo, gestione, controllo, consulenza e garanzia. Si ricordi che la classificazione riguarda la materia, non l'autore del documento, non le funzioni, ma il funzionamento dell'organo.**	
Consiglio e cariche istituzionali	**Riunione del gg/mm/aaaa**	Affare o attività	contiene i documenti relativi agli argomenti indicati in ODG e una copia di Convocazione, delibere e verbali	fascicolo per riunione
	Delibere di Consiglio	repertorio	contiene tutte le delibere e determine del consiglio direttivo, in ordine progressivo, per l'anno in corso	repertorio
	Delibere presidenziali	repertorio	delibere di urgenza del presidente, da ratificare in consiglio direttivo	repertorio
	convocazioni del consiglio direttivo	repertorio	contiene tutte le convocazioni e relativi ODG, in ordine progressivo, del consiglio direttivo per l'anno in corso	repertorio
	Consiglio Direttivo AAAA/AAAA	Affare o attività	comprende documenti residuali come per es. le dichiarazioni dei componenti relative alla trasparenza amministrativa, adempimenti fiscali e altro	fascicolo per mandato
	verbali del consiglio direttivo	repertorio	contiene tutti i verbali del consiglio direttivo, in ordine progressivo, per l'anno in corso	repertorio . Si apre con l'approvazione del primo verbale dell'anno e si chiude (l'anno successivo?) con l'approvazione del verbale dell'ultimo consiglio
Collegio Revisori dei Conti	**Riunione del gg/mm/aaaa**	Affare o attività	contiene i documenti relativi agli argomenti indicati in ODG e una copia di Convocazione e verbali	fascicolo per riunione
	convocazioni del Collegio Revisori dei Conti	repertorio	convocazioni in ordine progressivo	repertorio
	verbali del Collegio Revisori dei Conti	repertorio	verbali in ordine progressivo	repertorio
	Collegio dei revisori AAAA/AAAA	Affare o attività	comprende documenti residuali come per es. le dichiarazioni dei componenti relative alla trasparenza amministrativa, adempimenti fiscali e altro	fascicolo per mandato
Commissione Albo Medici Chirurghi	**Riunione del gg/mm/aaaa**	Affare o attività	contiene i documenti relativi agli argomenti indicati in ODG e una copia di Convocazione e verbali – da verificare eventuali connessioni con la classe dei procedimenti disciplinari	fascicolo per riunione
	Delibere della Commissione Albo Medici Chirurghi	repertorio	contiene tutte le delibere, in ordine progressivo, per l'anno in corso	repertorio
	convocazioni della Commissione Albo Medici Chirurghi	repertorio	convocazioni in ordine progressivo	repertorio
	verbali della Commissione Albo Medici Chirurghi	repertorio	verbali in ordine progressivo	repertorio
	Riunione del gg/mm/aaaa	Affare o attività	contiene i documenti relativi agli argomenti indicati in ODG e una copia di Convocazione e verbali	fascicolo per riunione

Commissione Albo Odontoiatri	**Delibere della Commissione Albo Odontoiatri**	repertorio	delibere in ordine progressivo	repertorio
	convocazioni della Commissione Albo Odontoiatri	repertorio	convocazioni in ordine progressivo	repertorio
	Commissione Albo Odontoiatri AAAA/AAAA	Affare o attività	comprende documenti residuali come per es. le dichiarazioni dei componenti relative alla trasparenza amministrativa, adempimenti fiscali e altro	fascicolo per mandato
	verbali della Commissione Albo Odontoiatri	repertorio	verbali in ordine progressivo	repertorio
Commissione Pari Opportunità	**Riunioni convocazioni e verbali e del gg/mm/aaaa**	Affare o attività	contiene i documenti relativi alla riunione (convocazioni e verbali)	fascicolo per riunione
Commissione per le medicine complementari	**Riunioni convocazioni e verbali**	Affare o attività	contiene i documenti relativi alle convocazioni e verbali	fascicolo per riunione
Gruppi di lavoro e altre commissioni	**Riunioni convocazioni e verbali xxx**	Affare o attività	contiene i documenti relativi alle convocazioni e verbali	fascicolo per riunione (per ogni commissione)
Rappresentanza dell'Ordine presso Enti, Istituzioni e assimilati	**FNOMCeO**	Affare o attività	Attività varie effettuate dal Consiglio e dai suoi componenti in rappresentanza dell'ente	fascicolo annuale
	Convocazioni e verbali Consiglio Nazionale FNOMCeO	Affare o attività	convocazioni e verbali in ordine progressivo	fascicolo annuale
	Convocazioni e verbali/decisioni Comitato Centrale FNOMCeO	Affare o attività	convocazioni e verbali in ordine progressivo	fascicolo annuale
	ENPAM	Affare o attività	Attività varie effettuate dal Consiglio e dai suoi componenti in rappresentanza dell'ente	fascicolo annuale
	Convocazioni e verbali Consiglio Nazionale ENPAM	Affare o attività	convocazioni e verbali in ordine progressivo	fascicolo annuale
	Fascicolo con denominazione dell'Ente/Istituzione	Affare o attività	Attività varie effettuate dal Consiglio e dai suoi componenti in rappresentanza dell'ente presso altre istituzioni	fascicolo annuale per ente
Arbitrati, Nomine e Designazioni	**Arbitrato xxx vs yyy**	Procedimento	documenti relativi ad arbitrati con intervento dell'Ordine	Fascicolo per ogni arbitrato
	Designazione/Nomina xxx	Procedimento amministrativo	documenti relativi a nomine e designazioni effettuate dall'Ordine in commissioni esterne all'Ente	Fascicolo per designazione/nomina
Assemblee ordinaria straordinaria ed elettorale		Affare o attività	Tutte le attività connesse all'Assemblea Ordinaria, all'Assemblea straordinaria, all'Assemblea Elettorale degli organi Istituzionali: convocazioni, verbali, etc…	fascicolo per assemblea
	Assemblea straordinaria del gg/mm/aaaa	Affare o attività		fascicolo per assemblea
	Assemblea elettorale del gg/mm/aaaa	Affare o attività		un fascicolo per ogni convocazione
Federazione Regionale degli Ordini dei Medici Chirurghi e degli Odontoiatri	**Attività della Federazione Regionale degli Ordini dei Medici Chirurghi e degli Odontoiatri**	Affare o attività	Comprende le attività e i documenti prodotti dalla Federazione regionale degli Ordini comprese quelle del Comitato Federativo (comprese convocazioni - delibere e verbali)	fascicolo annuale
	Attività della Commissione Regionale Albo Odontoiatri	Affare o attività	Comprende le attività e i documenti prodotti dalla Commissione Regionale Albo Odontoiatri (convocazioni delibere e verbali)	fascicolo annuale
Osservatori, indagini, studi e pubblicazioni	**Osservatori, indagini, studi e pubblicazioni**	Affare o attività	Comprende eventuali STUDI interni o esterni effettuati da gruppi di lavoro istituiti ad hoc per l'approfondimento di determinate materie.	fascicolo annuale

			Questo titolo riguarda la gestione delle posizioni degli iscritti all'Ordine per quanto concerne l'esercizio professionale, sia a livello di tenuta dell'Albo sia più nel dettaglio nella gestione delle ulteriori posizioni riferite genericamente non solo al fascicolo dell'iscritto, ma alla sua posizione professionale in ogni contesto

03 Tenuta Albi	**Comunicazioni massive su Tenuta Albi**	Affare o attività	Contiene le comunicazioni in entrata/uscita massive sulla verifica delle autocertificazioni presentate dagli iscritti (titoli, casellario giudiziale, altre competenze etc) e altri dati di interesse per la gestione dell'Albo, non autocertificati dagli iscritti (es. elenco iscritti certificabili ECM inviato da cogeaps) Qualora la comunicazione contenga documenti singoli, questi vanno associati al fascicolo personale dei ogni iscritto. Nel caso in cui il documento sia costituito da un unico elenco con più nominativi, sia associa l'intero elenco, sincerandosi di garantire la riservatezza di eventuali dati personali.	Fascicolo annuale
	Cognome Nome dell'iscritto.	Persona		Durata illimitata si apre con l'iscrizione del soggetto e si chiude con la cancellazione dall'Albo

Albo Medici chirurghi	**Dati istituzionali (1)**		Raccoglie tutta la documentazione inerente l'iscritto con particolare riferimento alla normativa vigente: Legge istitutiva D.L.C.P.S. 13 settembre 1946 n. 233 e s.m.i., D.P.R. 5 aprile 1950, n. 221, Elenchi Speciali: Abilitaz. eserc. med. gen. (D.M.15/12/1994), AGOPUNTURA - ANTROPOSOFIA - FITOTERAPIA - OMEOPATIA - OMOTOSSICOLOGIA (Accordo Stato-Regioni e Provincie Autonome 07/02/2013), Esperto qualificato radiologia (D.P.R.185/94), Titolo formaz. medicina generale (ex art. 30 Legge 368/99), Medico-chirurgo annot. (Ex art 5 Legge 409/85), Med. autorizzato radiologia (D.P.R.185/94 D.L.gs 230/95), Medico autorizzato Radioprotezione (D.Lgs 187/2000), Igiene medicina prevent. (Legge 1 art 1/bis 8/1/2002), Medico di Bordo (R.D.29/9/1895 n.636), Medico Immatr. (D.Lgs 386/98), Medico psicoterapeuta (Legge 56/89), Medico Universitario / Professore (art. 11 del D.P.R. 11 luglio 1980 n. 382), Med. Comp. Professionista con titoli idonei (D.Lgs 81/2008), Titolo formaz. medicina generale (D.Lgs 368 art. 29 17/8/1999), Titolo formaz. medicina generale (D.M. 10/10/88), Titolo formaz. medicina generale (D.Lgs 256/91), Titolo formaz. medicina generale (D.Lgs 206 art.36 del 9/11/2007 - Direttiva 2005/36/CE del 7/9/2005), Med. Compet. Lavoro art. 3 (D.Lgs 626/94), Med. Compet. Lavoro (art 55 D.Lgs 277/91), Tutors Valutatore (D.M. n. 445 19/10/2001). Vanno inserite tutte le istanze e documenti di: Iscrizione, Cancellazione, Trasfrimento, Inserimento in Elenchi speciali, Adempimenti ECM, le Autocertificazioni e relativa doicumentazione di verifica, DURC ENPAM	Durata illimitata si apre con l'iscrizione del soggetto e si chiude con la cancellazione dall'albo
	Qualifiche e attività (2)		Comprende le qualifiche professionali intese come attività svolta dall'iscritto e le comunicazioni dei conferimenti incarichi da parte delle Aziende (MMG, PLS, ecc.), comunicazioni di docenze da parte delle università (escluse quelle previste dall'art. 11 del D.P.R. 11 luglio 1980 n. 382), comunicazioni di assunzione di incarico di direttore sanitario di strutture pubbliche e private, incarichi ospedalieri, disponibilità a fare sostituzioni, documentazione relativa alle istanze presentate ai tribunali per l'iscrizione all'Albo CTU e all'albo dei Consulenti Tecnici d'Ufficio con relativi curricula (si inseriscono qui anche le convocazioni delle commissioni esaminatrici del Tribunale per la valutazione della richiesta e le deleghe del Presidente a presenziare alla Commissione); richieste/rilascio delle credenziali di accesso al Sistema TS, comunicazioni/richieste attivazione degli indirizzi PEC, richieste/rilascio dei certificati di iscrizione e di Good Standing e per pratiche di adozione, documentazione richiesta da terzi per la verifica delle autocertificazioni, richieste di informazioni sulla tenuta dell'Albo ; comunicazioni relative a smarrimenti/furti di tesserino, timbri, ricettari (anche da parte della Regione e/o Aziende Ulss). Rientrano in questo sottofascicolo anche l'aggiornamento professionale e l' ECM, con particolare riferimento alle richieste di inserimento dei crediti conseguiti come tutor per esami di stato, con Fad della Fnomceo o altri provider, richieste inserimento esoneri/esenzioni.	Durata illimitata si apre con l'iscrizione del soggetto e si chiude con la cancellazione dall'albo

Albo Odontoiatri	**Cognome Nome dell'iscritto. Al suo interno si trovano due**	Fascicolo di Persona		Durata illimitata si apre con l'iscrizione del soggetto e si chiude con la cancellazione dall'albo
	Dati istituzionali (1)		Raccoglie tutta la documentazione inerente l'iscritto con particolare riferimento alla normativa vigente: Legge istitutiva D.L.C.P.S. 13 settembre 1946 n. 233 e s.m.i., D.P.R. 5 aprile 1950, n. 221, Elenchi Speciali: AGOPUNTURA - ANTROPOSOFIA - FITOTERAPIA - OMEOPATIA - OMOTOSSICOLOGIA (Accordo Stato-Regioni e Provincie Autonome 07/02/2013), Elenco dentisti ex art 20 (Legge 409/85 - Profughi), Medico-chirurgo annot. (Ex art 5 Legge 409/85), Medico iscritto solo albo odo. (art. 4 Legge 409/85), Medico Universitario / Professore (art. 11 del D.P.R. 11 luglio 1980 n. 382). Vanno inserite tutte le istanze e documenti di: Iscrizione, Cancellazione, Trasfrimento, Inserimento in Elenchi speciali, Adempimenti ECM, le Autocertificazioni e relativa doicumentazione di verifica, DURC ENPAM	Durata illimitata si apre con l'iscrizione del soggetto e si chiude con la cancellazione dall'albo
	Qualifiche e attività (2)		Comprende le qualifiche professionali intese come attività svolta dall'iscritto e le comunicazioni dei conferimenti incarichi da parte delle Aziende (MMG, PLS, ecc.), comunicazioni di docenze da parte delle università (escluse quelle previste dall'art. 11 del D.P.R. 11 luglio 1980 n. 382), comunicazioni di assunzione di incarico di direttore sanitario di strutture pubbliche e private, incarichi ospedalieri, disponibilità a fare sostituzioni, documentazione relativa alle istanze presentate ai tribunali per l'iscrizione all'Albo CTU e all'albo dei Consulenti Tecnici d'Ufficio con relativi curricula (si inseriscono qui anche le convocazioni delle commissioni esaminatrici del Tribunale per la valutazione della richiesta e le deleghe del Presidente a presenziare alla Commissione); richieste/rilascio delle credenziali di accesso al Sistema TS, comunicazioni/richieste attivazione degli indirizzi PEC, richieste/rilascio dei certificati di iscrizione e di Good Standing e per pratiche di adozione, documentazione richiesta da terzi per la verifica delle autocertificazioni, richieste di informazioni sulla tenuta dell'Albo ; comunicazioni relative a smarrimenti/furti di tesserino, timbri, ricettari (anche da parte della Regione e/o Aziende Ulss). Rientrano in questo sottofascicolo anche l'aggiornamento professionale e l' ECM, con particolare riferimento alle richieste di inserimento dei crediti conseguiti come tutor per esami di stato, con Fad della Fnomceo o altri provider, richieste inserimento esoneri/esenzioni.	Durata illimitata si apre con l'iscrizione del soggetto e si chiude con la cancellazione dall'albo
			Per le società tra professionisti, l'art. 10 della legge 183/2011 al comma 5 prescrive che: "la denominazione sociale, in qualunque modo formata, deve contenere l'indicazione di società tra professionisti". Tale formulazione, identica a quella contenuta dall'art. 2326 del codice civile che enuncia: "La denominazione sociale, in qualunque modo formata, deve contenere l'indicazione di società per azioni" impone alle società tra professionisti di informare i terzi, attraverso il proprio nome commerciale, che la società costituita è una società tra professionisti, creando in tal modo una netta distinzione rispetto alle società che	

Albo Società tra Professionisti	**Denominazione della società**	fascicolo di persona giuridica	Raccoglie tutta la documentazione inerente la società in riferimento alla normativa vigente: D.L.C.P.S. 13 settembre 1946 n. 233 e s.m.i., D.P.R. 5 aprile 1950, n. 221 - -Legge n. 183 del 12/11/2011 - Decreto Ministero della Giustizia n. 34 del 08/02/2013 Regolamento in materia di società per l'esercizio di attività professionali regolamentate nel sistema ordinistico, ai sensi dell'art. 10 comma 10 della legge 12/11/2011 n. 183 - DPR n. 137 del 07/08/2012 art. 3. Contiene la domanda di iscrizione in bollo con con allegati :1) atto costitutivo e statuto della società in copia autenticata o nel caso di società semplice, dichiarazione autentica del socio professionista, cui spetti l'amministrazione della società; 2) elenco nominativo: a) dei soci che hanno la rappresentanza; b) dei soci iscritti all'Albo; c) degli altri soci con indicazione, in caso di altri professionisti, dell'Albo di appartenenza. 3) certificato di iscrizione all'Albo dei soci iscritti in altri Ordini o Collegi o autocertificazione; 4) certificato di iscrizione nella sezione speciale del registro delle imprese; 5) dichiarazione di insussistenza di incompatibilità di cui all'art. 6 del D.M. 8 febbraio 2013 n. 34; 6) Ricevuta del versamento della tassa di concessione governativa e della quota di iscrizione all'Albo.	Durata illimitata si apre con l'iscrizione del soggetto e si chiude con la cancellazione dall'albo
Prestazione di servizio Medici e Odontoiatri stranieri	**Prestazioni medici stranieri**	Affare o attività	Raccoglie tutta la documentazione inerente il sanitario straniero con particolare riferimento alla normativa vigente: art. 9 D.L.gs n. 206 del 9/11/2007, art.15 comma 2 Legge n. 3 del 11/1/2018 (che ha aggiunto	fascicolo annuale
	Prestazioni odontoiatri stranieri	Affare o attività	Raccoglie tutta la documentazione inerente il sanitario straniero con particolare riferimento alla normativa vigente: art. 9 D.L.gs n. 206 del 9/11/2007, art.15 comma 2 Legge n. 3 del 11/1/2018 (che ha aggiunto al D.L.gs n. 286 del 25/7/1998, l'art. 39 ter)	fascicolo annuale
Comunicazioni relative alla tenuta degli albi	**Comunicazioni da altri OMCeO**	Affare o attività	Raccoglie le comunicazioni inerenti le iscrizioni, cancellazioni, variazioni anagrafiche degli iscritti agli altri ordini dei medici	fascicolo annuale
	Comunicazioni da altri soggetti non OMCeO	Affare o attività	Comunicazioni generiche non riconducibili a singoli iscritti e ai relativi fascicoli personali	fascicolo annuale
Professione medica e odontoiatrica (circolari, regolamenti e norme)	**Circolari Regolamenti e Norme sull' Esercizio della professione medica**	Affare o attività	Raccoglie tutte le comunicazioni/circolari inerenti l'esercizio della professione	fascicolo annuale
	Circolari Regolamenti e Norme sull' Esercizio della professione odontoiatrica	Affare o attività	Raccoglie tutte le comunicazioni/circolari inerenti l'esercizio della professione	fascicolo annuale
Segnalazioni e Procedimenti disciplinari	**Codice identificativo procedimento Cognome Nome**	Procedimento amministrativo	Raccoglie tutta la documentazione riferita a segnalazioni nei confronti di un iscritto (da parte di iscritti, cittadini, aziende, altri ordini, ecc) e conseguenti convocazioni / audizioni con verbale, svolte in fase pre-disciplinare o per chiarimenti di varia natura e tutto l'iter del procedimento disciplinare, dall'apertura alla chiusura definitiva.	fascicolo per procedimento
	Segnalazioni nei confronti di iscritti ad altri Ordini	Affare o attività	documentazione relativa a segnalazione verso iscritti ad altri OMCeO, da inoltrare all'Ordine di competenza	fascicolo annuale
Flussi documentali FNOMCeO ed ENPAM	**Flussi Documentali Fnomceo/ENPAM**	Affare o attività	File .xml inviati tramite l'applicativo	fascicolo annuale
04 Tutela della professione e rapporti con gli Iscritti			**Questo titolo raccoglie le voci relative alla gestione dei rapporti, dei servizi, delle comunicazioni concernenti l'esercizio della professione non riconducibili al fascicolo dell'iscritto.**	

Quesiti e Istanze	**quesito da parte di xxx su yyy**	affare o attività	Quesiti e richieste di pareri sui temi generali della professione sia da parte degli iscritti che da altri soggetti. Comprende quesiti rivolti a FNOMCeO dagli Ordini o da terzi con relative risposte ed eventuali commenti e/o prese di posizione. Nel caso in cui il quesito o l'istanza riguardi l'amministrazione generale dell'ente deve confluire nella voce	per argomento
	istanze da parte di iscritti all'Ordine	affare o attività	raccoglie richieste varie da parte di iscritti	fascicolo annuale
	istanze da parte di soggetti NON iscritti all'Ordine	affare o attività	raccoglie richieste varie da parte di ALTRI soggetti	fascicolo annuale
Pubblicità dell'informazione sanitaria	**Pratiche pubblicità sanitarie (fascicolo unico per gli studi singoli e per le strutture)**	affare o attività	Riguarda pareri richiesti da iscritti e non iscritti, sulla pubblicità dell'informazione sanitaria sia del singolo professionista che della struttura sanitaria e relative risposte. **Per i singoli i documenti si associano al dossier dell'iscritto**	fascicolo annuale
	Pratiche di riconoscimento/pubblicizzazione di professionalità acquisite (fascicolo unico per tutte le richieste)	affare o attività	Raccoglie tutta la documentazione relativa alla richiesta da parte di Medici od Odontoiatri di riconoscimento di professionalità acquisite come previsto dalla legge 175/92 in materia di pubblicizzazione di competenze in assenza di titolo di specializzazione.	fascicolo annuale
Pareri di congruità parcelle e tariffario	**Richiesta parere di congruità percella sig. ….. (fascicolo per istanza)**	procedimento amministrativo	Raccoglie tutta la documentazione relativa alla richiesta e rilascio del parere di congruità delle parcelle da parte di Medici od Odontoiatri.	fascicolo per ogni richiesta
Autorizzazioni e accreditamento per l'attività professionale	**fascicolo per struttura o fascicolo annuale a seconda dell'organizzazione dell'attività**	affare o attività	In questa classe rientra la documentazione per gestire i rapporti con le strutture sanitarie (richiesta autorizzazione sanitaria, comunicazioni su direzione sanitaria). Non riguarda solo gli iscritti, ma anche la corrispondenza con gli enti preposti al rilascio e controllo delle stesse (Comune, Ulss, etc...).	fascicolo annuale?
Tutoraggi, tirocini e stage	**tirocinio per esame di abilitazione**	affare o attività	Raccoglie documentazione relativa allo svolgimento di attività di tutor per esami di stato	fascicolo annuale
	tirocinio V -VI anno medicina e chirurgia	affare o attività	Raccoglie documentazione relativa allo svolgimento di attività di tutor per il tirocinio del V e VI anno della facoltà di medicina	fascicolo annuale
	tirocinio CORSO MMG	affare o attività	Raccoglie documentazione relativa allo svolgimento di attività di tutor per il corso MMG	fascicolo annuale
Borse di studio e corsi MMG	**fascicolo per borsa di studio**	procedimento amministrativo	Pubblicazione bando di concorso per il triennio di formazione e borse di studio istituite dall'Ordine o da privati.	fascicolo per procedimento
	corso triennale MMG AAAA/AAAA	affare o attività	raccoglie documenti relativi al corso mmg comprese le nomine delle commissioni	fascicolo per la durata del corso
Servizi per gli iscritti	**Servizi vari (fascicolo unico) - se le attività lo richiedono è possibile aprire fascicoli dedicati**	affare o attività	Raccoglie documentazione relativa a rilascio dei contrassegni per auto, rilascio duplicati del tesserino, accordi con comune per parcheggio gratis la prima ora, eventuali convenzioni con alberghi, auto, agevolazioni per la banca o con professionisti per pareri gratuiti – richiesta appuntamenti per video-consulenza enpam e conferma degli stessi. Richiesta accesso a zona ZTL. Richieste di apertura partita iva. Richiesta elenco dei medici disponibili per le sostituzioni o manifestazioni sportive.	fascicolo annuale
Segnalazioni non riferite al singolo iscritto	**segnalazione nei confronti di xxx**	affare o attività	Segnalazioni riferite a soggetti che non sono medici/odontoiatri o che non riguardano la professione medica/odontoiatrica. In questa classe si inseriscono anche le sengnalazioni generiche nei confronti di reparti ospedalieri, servizi ASL, strutture sanitarie pubbliche e private, per le quali non è stato individuato un singolo soggetto al quale riferire l'esposto.	fascicolo per segnalazione, si apre con l'arrivo della segnalazione e si chiude con l'inoltro/archiviazione

05 Comunicazione, sistemi informativi			**Questo titolo è dedicato alle attività di comunicazione e di gestione dell'informazione dell'ente**	
Congressi e manifestazioni -	**accreditato ECM**	Affare o attività	Documentazione relativa all'evento organizzato	fascicolo per evento
	Richieste pubblicazione eventi	Affare o attività	Richieste di pubblicazione eventi su sito e/o bollettino dell'Ordine – richieste di diffusione eventi via email (se gestiti) - Corrispondenza relativa ai corsi FAD fnomceo e altri corsi ECM organizzati da altri Ordini o providers accreditati, di interesse per l'ente e gli iscritti.	fascicolo unico annuale
	Eventi istituzionali altri enti	Affare o attività	Inviti e corrispondenza relativi a eventi destinati agli organi istituzionali dell'Ordine a congressi ed eventi organizzati da altri Ordini e soggetti di diritto pubblico o privato	fascicolo unico annuale
Patrocini	**Richieste e concessioni patrocinio dell'Ordine**	Affare o attività	Comprende la documentazione relativa alla richiesta/rilascio del patrocinio dell'Ordine	fascicolo unico annuale in caso di sola documentazione di richiesta/concessione – fascicolo per evento in caso di procedura più estesa
Comunicazione, informazione -	**Ufficio stampa**	Affare o attività	Raccolta dell'attività svolta dall'ufficio stampa (se presente).	fascicolo unico annuale
	Notiziario/Newsletter	Affare o attività	Documentazione relativa agli articoli da pubblicare sul bollettino cartaceo/online.	fascicolo unico annuale
	Gestione sito internet	Affare o attività	Documenti relativi alla gestione e aggiornamento del sito: pubblicazioni, aggiornamenti tecnici, grafici etc. La procedura di affidamento per la gestione a società esterne rientra in "procedure negoziate bandi e gare"	fascicolo unico annuale
	Richieste pubblicazione annunci	Affare o attività	Comprende le richieste di inserimento di annunci vari nel sito dell'Ordine ad esclusione degli eventi al 05.02. Se gli annunci vengono gestiti esclusivamente attraverso un unico canale (sito o notiziario) possono essere inserite nel relativo fascicolo.	fascicolo unico annuale
Comunicati stampa	**Comunicati stampa anno AAAA**	Repertorio	Repertorio annuale dei comunicati stampa dell'OMCeO	repertorio
Sistemi informatici	**Software gestione OMCeO**	Affare o attività	Attività connessa alla gestione e aggiornamento dei software in uso all'Ordine. L'affidamento della fornitura rientra in "procedure	fascicolo unico annuale
	Gestione banche dati e servizi on live	Affare o attività	Attività connessa alla gestione delle banche dati e dei servizi on line a cui il personale o i rappresentanti dell'ente accedono per l'esercizio delle attività istituzionali	fascicolo unico annuale
	Hardware gestione OMCeO	Affare o attività	Attività connessa alla gestione e aggiornamento dei sistem hardware in uso all'Ordine. L'affidamento della fornitura rientra in "procedure negoziate bandi e gare"	fascicolo unico annuale
06 Risorse umane			**Questo titolo è dedicato alle funzioni relative alla gestione del personale, sia esso dipendente interno o esterno (collaboratori a qualsiasi titolo). Per i documenti relativi a ciascun dipendente viene istruito un fascicolo nominativo. Le disposizioni nomative generali sul pesonale sono inserite nell'amministrazione generale dell'Ente (01.03)**	
Concorsi Selezioni e colloqui	**Selezione per assunzione personale**	Procedimento amministrativo	Raccoglie tutta la documentazione inerente la procedura concorsuale (avviso, domande di partecipazione, verbali, graduatorie….)	fascicolo per procedimento
Collaborazioni esterne e Stage	**Selezione per incarico o stage**	Procedimento amministrativo	Raccoglie tutta la documentazione inerente la selezione di personale per incarichi di collaborazione o stage	fascicolo per procedimento
Trattamento (posizione) giuridico ed economico del dipendente	**Fascicolo di persona (nome dipendente)**	Affare o attività	Raccoglie tutta la documentazione riferita alla posizione giuridica ed economica del dipendente (contratto di lavoro, mobilità, comandi, infortuni, richiesta ferie, permessi…formazione e procedimenti disciplinari)	fascicolo di persona
Tutela della salute e sicurezza sul luogo di lavoro	**adempimenti salute e sicurezza sul lavoro**	Affare o attività	raccoglie le eventuali prescrizioni dettate dal RSPP non riferite al singolo dipendente e non riferito alla struttura	fascicolo unico annuale

Giudizi, responsabilità e provvedimenti disciplinari e contenzioso	**Fascicolo con la denominazione del procedimento e il nominativo del dipendente a cui è riferito**	Procedimento amministrativo	documentazione relativa al caso in oggetto	fascicolo per procedimento
Formazione e aggiornamento professionale	**corsi di formazione del personale**	Affare o attività	documenti e circolari su corsi di formazione rivolti al personale da FNOMCEO o altri soggetti pubblici o privati	fascicolo unico annuale
07 Risorse Finanziarie, Patrimoniali e strumentali			**In questo titolo rientrano le funzioni attribuite dalla legge agli Ordini in materia di disponibilità di risorse finanziarie e di gestione contabile, quelle relative alla titolarità e alla gestione del patrimonio dell'Ordine, mobile ed immobile, nonchè quelle relative alla acquisizione e gestione dei beni e servizi strumentali allo svolgimento delle attività e funzioni finali. Talune attività del titolo sono state indicate adottando la terminologia dell'atto finale.**	
Bilanci, Variazioni di Bilancio, Rendiconti.	**Rendiconto della gestione economica e finanziaria anno …..**	Affare o attività	Le attività riferite a questo fascicolo riguardano i documenti contabili prodotti ex lege ed approvati dai competenti organi ed eventuali documenti preparatori. La relazione previsionale e programmatica. Il Piano degli acquisti. Possono essere associati documenti secondari come le delibere di approvazione di Consiglio e di Assemblea, la relazione del Presidente, del Tesoriere e quella dei Revisori dei Conti. Articolato in Conto Consuntivo anno precedente, Bilancio di Previsione anno corrente, Variazioni al bilancio di previsione. Stato patrimoniale e Conto economico. Si apre con i deliberati di Consiglio di approvazione dei vari documenti e si chiude con le relative approvazioni assembleari. In questo fascicolo possono essere inserite le comunicazioni da e per Fnomceo sul numero di iscritti a ruolo per l'erogazione della quota di spettanza ed eventuali richieste di verifica.	fascicolo annuale
Contratti, Incarichi e Collaborazioni professionali	**Affidamento incarico (nome)**	Affare o attività	Attività connesse alla gestione dell'affidamento o incarico consistenti in corrispondenza varia compresi i preavvisi di parcella, variazioni di condizioni contrattuali con banche, posta, assicurazioni ecc.	Il fascicolo viene aperto a seguito della conclusione della procedura negoziata o gara con l'affidamento dell'incarico che può avvenire mediante sottoscrizione di un contratto o con lettera di incarico secondo gli usi. Contiene tutta la
	Collaborazione professionale (nome)	Affare o attività		
	Registro dei contratti	repertorio	registro dei contratti stipulati dall'Ordine per incarichi, consulenze, etc.	repertorio
Procedure negoziate, bandi e gare	**Procedura negoziata per ….. (specificare per quale attività)**	Procedimento amministrativo	Attività connesse alla procedura (vedi scheda di mappatura). Il fascicolo viene aperto con l'acquisizione del Cig e successivamente con il documento che avvia la procedura scelta (es. manifestazione di interesse, richiesta preventivi, bando). Contiene tutta la documentazione relativa alla procedura (documentazione di partecipazione alla manifestazione, produzione di preventivi, nomina commissione aggiudicatrice, verbali di commissione, verifica requisiti,	fascicolo per procedimento
	Affidamenti diretti	Procedimento amministrativo	contiene i documenti relativi agli acquisti diretti su MEPA/altre piattaforme, che non comportano particolari complessità e si esauriscono con determina a contrarre + ordinativo.	fascicolo annuale
Fatture PA (e note di credito)	**Registro delle Fatture**	REGISTRO DELLE FATTURE		Gestione automatizzata
Notifiche SDI	**Registro delle Notifche**	REGISTRO DELLE NOTIFICHE		Gestione automatizzata
	gestione incasso quota ordine	Affare o attività	Procedura connessa alla gestione dell'incasso delle quota come concordata con il gestore. Il fascicolo si apre con la comunicazione al gestore della riscossione degli elenchi iscritti a ruolo e comprende tutte le comunicazioni sulla gestione dei medesimi (inclusi mandati di addebito, variazioni iban, ricevute, corrispondenza varia con il gestore	fascicolo annuale

Gestione delle entrate e riscossioni	gestione morosi	Affare o attività	Il fascicolo si apre con il primo sollecito e si chiude con l'eventuale cancellazione ex art. 11 (i documenti relativi al singolo iscritto saranno inseriti anche nel dossier)	fascicolo annuale
	Erogazione contributi ordinari e straordinari da Enpam e Fnomceo	Affare o attività	Comunicazioni relative alla modalità di erogazione da parte degli Enti e successiva richiesta e documenti vari di gestione .Il fascicolo si apre e si chiude con la richiesta del relativo contributo e l'erogazione dello stesso	Fascicolo per ogni richiesta di contributo
	entrate diverse (affitto locali, convenzioni, contributi di altri enti)	Affare o attività	documenti relativi alla gestione delle entrate per finalità diverse da quelle dei fascicoli precedenti	fascicolo annuale
Gestione delle uscite	Rimborsi degli Organi Istituzionali, gruppi di lavoro e commissioni	Affare o attività	comprende le richieste di rimborso varie e le dichiarazioni di accettazione/rinuncia degli emolumenti connessi alla carica	fascicolo annuale
	Adempimenti fiscali, contributivi e assicurativi	Affare o attività	comprende avvisi/ ricevute dei pagamenti (Tassa rifiuti, Irpef, polizze, ecc.)	fascicolo annuale
	Gestione cassa economale	Affare o attività	documentazione relativa alla gestione della cassa economale	fascicolo annuale
O.I.L. Ordinativi Elettronici Tesoreria	gestione dell'attività di tesoreria	Affare o attività		si apre con il primo ordinativo
Beni Mobili e Immobili (compresi accessori informatici)	Registro dei cespiti e inventario	Affare o attività	Il fascicolo si apre e si chiude con l'approvazione del documento	fascicolo per attività
Mutui	Mutuo per xxx con (nome istituto bancario)	Affare o attività	tutta l'attività di apertura, gestione e chiusura . Si apre con il contratto bancario di mutuo	Fascicolo per ogni mutuo
8 Previdenza			**Comprende tutta l'attività previdenziale e assistenziale riferita agli iscritti e ai superstiti per conto dell'Ente di previdenza.**	
	Pratiche Fondo Generale Quota A e Quota B	Affare o attività	I vari fascicoli raccolgono le pratiche riferite ai singoli iscritti inviate dall'ordine all'Enpam . Tutti i fascicoli si aprono con la prima richiesta e sono annuali. Il documento sarà poi inserito nel dossier dell'iscritto	fascicolo annuale
	Pratiche Fondi Speciali MMG - PLS Continuità assistenziale - Specialisti Ambulatoriali -Medicina dei Servizi	Affare o attività		
	Pratiche di invalidità Fondo Generale	Affare o attività		
	Pratiche Assistenza - Sussidi - Reversibilità e varie	Affare o attività		
	Autorizzazione all'accesso ai servizi on-line offerti dalla Fondazione Enpam	Affare o attività		
	Comunicazioni su gestione ENPAM	Affare o attività	comunicazioni riguardanti la gestione istituzionale e normativa dell'enpam	fascicolo annuale
Commissione Invalidità ENPAM	Nomina dei Componenti la Commissione Invalidità	Affare o attività	Inerente all'attività di gestione delle nomina e variazioni della Commissione invalidità. Il fascicolo si apre all'inizio del mandato di Consiglio con la nomina dei componenti	fascicolo per durata del mandato della commissione
	Attività della Commissione Invalidità	Affare o attività	Raccoglie i documenti relativi a tutte le attività svolte dalla Commissione quali convocazioni, verbali ed eventuale corrispondenza con il richiedente. Comprende anche la rendicontazione delle riunioni per il calcolo delle spettanze di Enpam. Il fascicolo si apre con la prima convocazione della commissione	fascicolo per durata del mandato della commissione
Varie altri enti previdenziali e assistenziali	Fascicolo Onaosi	Affare o attività	Raccoglie i documenti relativi all'attività dell'Onaosi nei confronti dell'ordine e degli iscritti	fascicolo annuale
09 Relazioni istituzionali con altri Enti ed Associazioni			**Questo titolo è stato creato per dare autonomia ad una serie di relazioni istituzionali intercorrenti con alcuni soggetti particolari, per evidenziarne la peculiarità, quindi ogni Ordine dovrà valutare individualmente l'organizzazione di questi documenti**	

Altri ordini e collegi professionali Medici e non medici	**Comunicazioni varie altri OMCeO**	Affare o attività	Raccoglie comunicazioni di cambi sede e recapiti - comunicazioni varie non previste in altri punti relative a OMCeO	fascicolo annuale
	Comunicazioni varie altri Ordini e collegi NON medici	Affare o attività	Raccoglie comunicazioni di cambi sede e recapiti - comunicazioni varie non previste in altri punti relative ad altri Ordini e collegi NON medici	fascicolo annuale
Relazioni istituzionali con soggetti di diritto pubblico	**Fascicolo con denominazione del soggetto**	Affare o attività	Raccoglie la documentazione relativa a eventuali rapporti con soggetti di diritto pubblico (comuni, regioni, università, scuole, province etc) che non comportano una rappresentanza stabile dell'Ordine A seconda della complessità dell'attività posta in essere si può creare un fascicolo specifico	Fascicolo annuale / fascicolo per attività
Relazioni istituzionali con soggetti di diritto privato	**Fascicolo con denominazione del soggetto**	Affare o attività	Raccoglie la documentazione relativa a eventuali rapporti con soggetti di diritto privato (associazioni di volontariato, culturali, sindacali, imprese etc)	fascicolo annuale
Aggregazioni territoriali Mediche (UTAP – medicine di gruppo)	**Medicine di Gruppo**	Affare o attività	Raccoglie comunicazioni relative ad attivazione/modifica/chiusura di medicine di gruppo, UTAP, medicina in rete e pediatria di gruppo.	fascicolo annuale – i documenti si associano anche al dossier degli iscritti
Elezioni e nomine altri enti	**Elezioni e nomine altri Enti**	Affare o attività	Fascicolo dedicato alle comunicazioni relative a Enti diversi dagli	fascicolo annuale
	Elezioni e nomine altri OMCeO	Affare o attività	Fascicolo dedicato esclusivamente alle comunicazioni relative a elezioni e cariche degli OMCeO italiani	fascicolo annuale
10 Risorse documentali			**Questo titolo è riferito alle gestioni documentali digitali previste dalla norma**	
Registro giornaliero di protocollo	**Registro giornaliero di protocollo**	Affare o attività	registro giornaliero	fascicolo annuale
Rapporti di versamento	**rapporti di versamento**	Affare o attività	contiene i rapporti di versamento inviati dal conservatore	fascicolo annuale
Gestione dell'archivio	**gestione archivio dell'Ordine**	Affare o attività	Riguarda pianificazione e revisione degli strumenti di gestione dell'archivio (piano di classificazione, di conservazione, manuale di gestione e manuale di conservazione). Riordinamento e inventariazione	fascicolo annuale
	Pratica di xxx sovrintendenza xxx	Affare o attività	Pratiche con sovrintendenza per approvazione titolario, scarto etc	fascicolo per attività
11 Affari Legali			**Si è deciso di prevedere un titolo specifico dedicato agli affari legali, nonostante l'obiezione che quasi sempre essi si inseriscono all'interno di un procedimento, per due motivi: prima di tutto perché la funzione si configura come eccezionale e straordinaria, poi perché talvolta le azioni legali, i pareri e le consulenze interessano materie diverse e possono rivestire carattere generale e/o preliminare a una pluralità di procedimenti concreti. Si è constatato che spesso i fascicoli di causa, si formano presso un professionista esterno, cui l'amministrazione ha affidato l'incarico di rappresentarla: in tal caso sarà cura dell'Ordine recuperare, una volta terminata la causa,i documenti, perché rimangano nella memoria dell'ente.**	
Contenzioso	**Denominazione della causa**	Affare o attività	Raccoglie i documenti relativi a tutta la causa	un fascicolo per ciascuna causa
Pareri e consulenze	**Pareri e consulenze**	Affare o attività	Raccoglie tutta l'attività di richiesta e gestione dei pareri e delle consulenze che l'ordine esprime a richiesta degli iscritti o di altri soggetti	Un fascicolo per ogni pareri /consulenze
Arbitrati	**Nomina componenti collegio arbitrale**	Procedimento amministrativo	Raccoglie i documenti relativi alla nomina e gestione del Collegio (nomina ed eventuali rimborsi/gettoni ecc.)	Un fascicolo relativo alla gestione del collegio arbitrale
	Fascicolo arbitrato ….	Procedimento amministrativo	Raccoglie tutti i documenti relativi al singolo arbitrato (richiesta di attivazione, convocazioni, verbali/pareri ecc.)	un fascicolo per ogni arbitrato

Allegato 8 A – Regolamento per la tutela delle persone fisiche con riguardo al trattamento dei dati personali

DELIBERAZIONE CD N. 32 DEL 12/01/2022

Allegato 8 B – Registro delle attività di trattamento

Modello per la raccolta di informazioni sulla violazione dei dati personali

(artt.4, 33, 34 del Regolamento (UE) 2016/679 – RGPD e art. 26 del d.lgs. 51/2018)

Sez. A - Dati del soggetto segnalante

Cognome: _____ Nome:_____
E-mail:_____
Recapito telefonico per eventuali comunicazioni:_____
Funzione:_____

Sez. B -Titolare del Trattamento

Denominazione[9]: Ordine provinciale dei Medici Chirurghi e degli Odontoiatri di

Codice Fiscale:
Indirizzo:
PEC:

Sez. B1- Ulteriori soggetti coinvolti nel trattamento

Indicare i riferimenti di ulteriori soggetti coinvolti ed il ruolo svolto (contitolare, responsabile del trattamento[10] rappresentante del titolare non stabilito nell'Ue)

Denominazione: _____
Codice Fiscale/P.IVA_____(indicare se Soggetto privo di C.F./P.IVA)
Ruolo: ☐ Contitolare ☐ Responsabile ☐ Rappresentante

Denominazione: _____
Codice Fiscale/P.IVA_____(indicare se Soggetto privo di C.F./P.IVA)
Ruolo: ☐ Contitolare ☐ Responsabile ☐ Rappresentante

9 Indicare nome e cognome nel caso di persona fisica.

10 In tale tipologia rientra anche il Responsabile individuato ai sensi art. 28, par. 4.

Denominazione: _____
Codice Fiscale/P.IVA_____(indicare se Soggetto privo di C.F./P.IVA)
Ruolo: ☐ Contitolare ☐ Responsabile ☐ Rappresentante

Sez. C - Informazioni di sintesi sulla violazione

Indicare quando è avvenuta la violazione

☐ Il _____
☐ Dal _____ (la violazione è ancora in corso)
☐ Dal _____ al _____
☐ In un tempo non ancora determinato

Ulteriori informazioni circa le date in cui è avvenuta la violazione

1. Breve descrizione della violazione

2. Natura della violazione

☐ a) Diffusione/accesso non autorizzato o accidentale [11]
☐ b) Modifica non autorizzata o accidentale [12]
☐ c) Impossibilità di accesso, perdita, distruzione non autorizzata o accidentale [13]

3. Causa della violazione

☐ Azione intenzionale interna

11. Perdita di confidenzialità

12. Perdita di integrità

13. Perdita di disponibilità

- ☐ Azione accidentale interna
- ☐ Azione intenzionale esterna
- ☐ Azione accidentale sterna
- ☐ Sconosciuta
- ☐ Altro (specificare)

4. Categorie di dati personali oggetto di violazione

- ☐ Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale, altro...)
- ☐ Dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile)
- ☐ Dati di accesso e di identificazione (username, password, customer ID, altro…)
- ☐ Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro…)
- ☐ Dati relativi alla fornitura di un servizio di comunicazione elettronica (dati di traffico, dati relativi alla navigazione Internet, altro…)
- ☐ Dati relativi a condanne penali e ai reati o a connesse misure di sicurezza o di prevenzione
- ☐ Dati di profilazione (elaborazione automatizzata dei dati personali)
- ☐ Dati relativi a documenti di identificazione/riconoscimento (carta di identità, passaporto, patente, CNS, altro…)
- ☐ Dati di localizzazione
- ☐ Dati che rivelino l'origine razziale etnica
- ☐ Dati che rivelino opinioni politiche
- ☐ Dati che rivelino convinzioni religiose o filosofiche
- ☐ Dati che rivelino l'appartenenza sindacale
- ☐ Dati relativi alla vita sessuale o all'orientamento sessuale
- ☐ Dati relativi alla salute
- ☐ Dati genetici
- ☐ Dati biometrici
- ☐ Categorie ancora non determinate
- ☐ Altro

5. Indicare il volume (anche approssimativo) dei dati personali oggetto di violazione[14]

- ☐ N. _____
- ☐ Circa n. _____
- ☐ Un Numero (ancora) non definito di dati

6. Categorie di interessati coinvolti nella violazione

- ☐ Dipendenti/Consulenti ecc.
- ☐ Utenti in genere
- ☐ Iscritti all'Ordine
- ☐ Soggetti che ricoprono incarichi istituzionali
- ☐ Beneficiari
- ☐ Pazienti
- ☐ Minori
- ☐ Persone vulnerabili (es. vittime di violenze o abusi, rifugiati, richiedenti asilo)
- ☐ Categorie ancora non determinate
- ☐ Altro (specificare)

- ☐ Eventuali ulteriori dettagli circa le categorie di interessati

7. Numero (anche approssimativo) di interessati coinvolti nella violazione

- ☐ N. _____ interessati
- ☐ Circa n. _____ interessati
- ☐ Un numero (ancora) sconosciuto di interessati

[14] Ad esempio, numero di referti, numero di record di un database, numero di transazioni registrate.

Sez. D - Informazioni di dettaglio sulla violazione[15]

1. **Descrizione dei sistemi e delle infrastrutture IT coinvolti nell'incidente, con indicazione della loro ubicazione**

- ☐ Computer
- ☐ Dispositivo mobile
- ☐ Documento cartaceo
- ☐ File o parte di file
- ☐ Strumento di back up
- ☐ Rete
- ☐ Altro:

2. **Misure di sicurezza tecniche e organizzative adottate per garantire la sicurezza dei dati, dei sistemi e delle infrastrutture IT coinvolti[16]**

a) Misure organizzative:

- ☐ Nomina per iscritto personale
- ☐ Istruzioni per il trattamento
- ☐ Formazione del personale
- ☐ Accesso controllato
- ☐ Armadi chiusi
- ☐ Procedura modifica credenziali
- ☐ Policy di Ateneo

b) Misure tecniche:

- ☐ Autenticazione
- ☐ Autorizzazione
- ☐ Cifratura dei dati
- ☐ Separazione
- ☐ Firewall
- ☐ Antivirus
- ☐ Business continuity
- ☐ Disaster recovery

[15] Segue punto 1, 2 e 3 della sez. C.

[16] Indicare le misure in essere al momento della violazione.

☐ Intrusion detection

☐ Vulnerability assessment/penetration test

Sez. E – Misure adottate a seguito della violazione

2. Misure tecniche e organizzative adottate (o di cui si propone l'adozione[17]) per porre rimedio alla violazione e ridurne gli effetti negativi per gli interessati

[17] Nella descrizione distinguere le misure adottate da quelle in corso di adozione.

Allegato 11 - Formati di File e riversamento dell'Ente

I formati di file e il riversamento dell'ente si riferiscono, rispettivamente, alla tipologia di file utilizzati per archiviare documenti e al processo di trasferimento di dati tra diversi enti o sistemi informatici. I formati di file, come PDF o DOCX, determinano la struttura e il contenuto dei documenti, mentre il riversamento assicura la corretta comunicazione e lo scambio di informazioni tra le parti coinvolte.

Formati di file:

I formati di file sono un aspetto fondamentale della gestione digitale dei documenti, soprattutto per quanto riguarda la loro conservazione e la loro interoperabilità. Alcuni dei formati più comuni includono:

- **PDF (Portable Document Format):**

Raccomandato per documenti destinati alla spedizione e alla conservazione, garantisce la fedeltà del formato e la leggibilità nel tempo.

- **PDF-A**
- **DOCX (Microsoft Word Open XML)**
- **TIFF (Tagged Image File Format)**
- **JPEG2000**
- **XML (Extensible Markup Language)**
- **TXT (Text)**
- **CSV (Comma Separated Values)**
- **JSON (JavaScript Object Notation)**
- **XLSX**
- **PPTX**
- **EML**
- **ODT**
- **FODT**
- **ODS**
- **FODS**
- **ODP**
- **FODP**
- **ODG**
- **FODG**
- **P7M**
- I file .MSG (Email Microsoft Outlook) saranno convertiti in .EML

Riversamento dell'ente:

Il riversamento dell'ente, o flusso di dati, è il processo che permette la trasmissione di dati tra diverse entità o sistemi informatici. Questo processo può essere utilizzato per:

- **Scambio di informazioni:**

Trasferire dati tra diverse amministrazioni pubbliche, ad esempio per lo scambio di dati anagrafici.

- **Autenticazione e verifica:**

Verificare l'autenticità dei documenti o degli scambi di dati, spesso attraverso l'utilizzo di firme digitali.

- **Tracciabilità:**

Monitorare il flusso di dati e i processi di trasferimento, garantendo la trasparenza e la sicurezza.

Considerazioni aggiuntive:

- La scelta del formato di file deve essere effettuata in base alle specifiche esigenze della gestione documentale, tenendo conto della tipologia di documento, del formato di destinazione e delle normative applicabili.
- Il riversamento dei dati deve essere effettuato in modo sicuro e protetto, garantendo la riservatezza e l'integrità delle informazioni.
- È importante adottare standard di interoperabilità e di scambio di dati che consentano una comunicazione fluida tra i diversi enti.

Allegato 12 – Documenti esclusi dal protocollo

Assegni e altri valori (senza lettera di accompagnamento).
Auguri, ringraziamenti, condoglianze, congratulazioni
Avviso di accettazione e avvenuta consegna PEC; ricevute di ritorno delle raccomandate
Bollettini ufficiali e notiziari delle pubbliche amministrazioni compresi quelli degli Ordini d'Italia, gazzette ufficiali; giornali e riviste; newsletter giuridica - centro studi di diritto sanitario e farmaceutico - rassegne stampa
Comunicati ONAOSI
Comunicati stampa FNOMCEO
Comunicazioni esiti aggiornamento INI-PEC
Atti preparatori interni per Convocazioni a incontri o riunioni interne
Curricula di persone che chiedono di lavorare all'Ordine
Distinta acquisto bolli e materiale postale
Estratti conto bancari e postali;
Invio nominativi per video consulenze ENPAM – deleghe e richieste duplicati CU
Inviti a manifestazioni che non attivino procedimenti amministrativi
Libri (a meno che non siano accompagnati da lettera di accompagnamento)
Materiali pubblicitari; pubblicità conoscitiva di convegni; pubblicità in generale; offerte preventivi e listini prezzi di terzi non richiesti
Notifiche tecniche automatizzate (es. notifiche di Irideweb/IrideOnline - acquisizione fatture IRIDEPLUS, esiti aggiornamento INIPEC)
Report mail in quarantena/ posta indesiderata
Richiesta pubblicazione concorsi - annunci di lavoro e annunci vari per la bacheca del sito; richiesta pubblicazione eventi fuori provincia (senza invito formale diretto al presidente)
Richieste di iscrizione ai corsi di aggiornamento dell'Ordine (canali web o altri) e relativi attestati ECM
Scambi di e-mail a carattere informale, paragonabili a conversazioni verbali, che non comportino costituzione o modifica di atti o documenti amministrativi (prenotazioni alberghi e biglietti treno/aereo per consigli nazionali e trasferte)
Scambio mail con consulente del lavoro, consulente legale, consulente fiscale

Registro di protocollo di emergenza

Codice registro (es. RE Ed.1-2025)	
Data apertura	
Motivazione	
Data chiusura	

Il presente registro di emergenza è attivato su autorizzazione del Responsabile della gestione documentale nominato dall'Ente

N. registrazione		Tipo	Data	Oggetto	Allegati	Classe documentale	Note
Codice registro	n. protocollo	**E**ntrata, **U**scita, **I**nterno			Numero allegati		
RE01-2025	0000001	E					
RE01-2025	0000002	U					
RE01-2025	0000003	E					
RE01-2025	0000004	E					
RE01-anno							
RE01-anno							

OMCeOCampobasso
Ordine Provinciale dei Medici-Chirurghi e degli Odontoiatri

DELIBERAZIONE N. 64/CD DEL 09/06/2025

OGGETTO: ISTITUZIONE DEL "SERVIZIO ARCHIVISTICO DELL'ORDINE" ED INDIVIDUAZIONE DEL RESPONSABILE DEL SERVIZIO

Il Consiglio Direttivo dell'Ordine dei Medici Chirurghi e degli Odontoiatri della Provincia di Campobasso, riunitosi in modalità mista nella seduta del 09/06/2025, così costituito:

Nome e cognome	Carica	Presente	Assente
Giuseppe De Gregorio	Presidente	X	
Giulietta Terranova	VicePresidente		X
Michela Musacchio	Segretario	X	
Sergio Torrente	Tesoriere	X*	
Biagio Apollonio	Componente	X*	
Patrizia Cartoccio	Componente		X
Domenico Coloccia	Componente (odont.)	X	
Federico Cutrone	Componente	X	
Antonia De Socio	Componente	X	
Federico Di Renzo	Componente	X	
Paola Di Rocco	Componente		X
Antonella Giordano	Componente	X*	
Germano Guerra	Componente	X*	
Roberta Sabusco	Componente (odont.)	X*	
Matteo Santamaria	Componente		X
Paolo Scarano	Componente	X	

*: In collegamento telematico

PREMESSO che il prossimo 30 giugno 2025 risulta essere il termine ultimo per adempiere all'aggiornamento e alla pubblicazione del "*Manuale di gestione documentale*", come da comunicazione pervenuta dalla FNOMCeO tramite nota PEC con Prot. N E-2025-0001124 del 09/06/2025;

PREMESSO che per tale incarico risulta necessaria la nomina del Responsabile della gestione documentale, come stabilito dal Piano Triennale per l'informatica nelle PA 2024-2026;

CONSIDERATO che ai sensi dell'Art. 61 del D.P.R. 445/2000, *Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa*, le Pubbliche Amministrazioni devono istituire "un servizio per la tenuta del protocollo informatico, dei flussi documentali e degli archivi", cui è preposto "un dirigente ovvero un funzionario (…) in possesso di idonei requisiti professionali o di professionalità tecnico-archivistica", che deve svolgere i compiti specificati al comma 3) e individuato, quale figura adatta a ricoprire tale incarico, il Funz. Amm.vo Dott.ssa Maria, Giuliana Zicchillo;

VISTO che per il funzionamento dell'attività è altresì indispensabile procedere all'istituzione di un Ufficio competente per la gestione del servizio in questione, cui demandare altri compiti definiti dall'Art. 61, co. 3, del D.P.R. 445/2000;

CONSIDERATO che il D.P.C.M. del 3 dicembre 2013 – "*Regole tecniche per il protocollo informatico…*" dispone la nomina di un Responsabile per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi e l'adozione, successivamente alla nomina del Responsabile del servizio e sulla Sua proposta, del "*Manuale di gestione*" definito rispettivamente all'Art. 5;

con votazione espressa all'unanimità dei presenti,

DELIBERA

A. di istituire l'Ufficio denominato "Servizio archivistico dell'Ordine" per la gestione informatica dei documenti, dei flussi documentali e degli archivi, di seguito e per semplificazione denominato "Ufficio";
B. di attribuire all'Ufficio i seguenti compiti:
    1. predisporre lo schema del Manuale di gestione di cui all'art. 5 delle Regole tecniche per il protocollo;
    2. curare la redazione e l'aggiornamento del Titolario, del Piano di fascicolazione e degli altri strumenti archivistici previsti;
    3. proporre i tempi, le modalità e le misure organizzative e tecniche finalizzare alla eliminazione dei protocolli di settore e di reparto, dei protocolli multipli e in più generale dei protocolli diversi dal protocollo informatico;
    4. predisporre il Piano per la sicurezza informatica relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici, nel rispetto delle misure di sicurezza previste nel disciplinare tecnico pubblicato in allegato B del D. Lgs. N. 196/2003 e ss.mm.ii. e dalla Circolare AgID del 18 aprile 2017 n. 2/201;
C. di riconoscere tra i compiti del Servizio:
    - abilitare gli addetti dell'Amministrazione all'utilizzo del sistema di protocollo informatico e definire per ciascuno di essi il tipo di funzioni disponibili (esempio: consultazione, registrazione, modifica, ecc.);
    - garantire il rispetto delle disposizioni normative durante le operazioni di registrazione e di segnatura di protocollo;
    - garantire la corretta produzione e conservazione del registro giornaliero di protocollo;

- curare le funzionalità del sistema affinché, in caso di guasti o anomalie, siano ripristinate entro 24 ore dal blocco delle attività e, comunque, nel più breve tempo possibile;
- conservare le copie di salvataggio delle informazioni del sistema di protocollo e del registro di emergenza in luoghi sicuri e diversi da quello in cui viene custodito il suddetto sistema;
- garantire il buon funzionamento degli strumenti e il rispetto delle procedure concernenti le attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali;
- autorizzare le operazioni di annullamento delle registrazioni di protocollo;
- aprire e chiudere il registro di emergenza;
- definire e assicurare i criteri uniformi di trattamento del documento informatico, di classificazione e archiviazione, nonché di comunicazione interna, ai sensi dell'art. 50, co.4, del T.U.;
- curare le attività di registrazione di protocollo affinché, in caso di guasti o anomalie, ne sia ripristinata la funzionalità entro 24 ore dal blocco o, comunque, nel più breve tempo possibile;
- autorizzare, aprire, chiudere ed assicurarsi della corretta compilazione dell'eventuale protocollo di emergenza;

D. di pubblicare la presente Deliberazione nella sezione "Amministrazione Trasparente" del sito istituzionale dell'Ordine.

La gestione dell'Ufficio è affidata al Funzionario Amministrativo Dott.ssa Maria, Giuliana Zicchillo, come persona in possesso di idonei requisiti professionali o di professionalità tecnico-archivistica, che pertanto avrà la responsabilità dei compiti descritti al punto B., che dovranno essere svolti di concerto con il personale della Segreteria.

Letto, firmato e sottoscritto.

IL SEGRETARIO
Dr.ssa Michela Musacchio

MICHELA
MUSACCHIO
12.06.2025 18:08:28
GMT+01:00

IL PRESIDENTE
Dr. Giuseppe De Gregorio

GIUSEPPE
DE
GREGORIO
12.06.2025
19:26:51
GMT+01:00

OMCeOCampobasso
Ordine Provinciale dei Medici-Chirurghi e degli Odontoiatri

DELIBERAZIONE N. 32/CD/2022 DEL 12/01/2022

OGGETTO: **REGOLAMENTO PER LA TUTELA DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI**

Il Consiglio Direttivo dell'Ordine dei medici chirurghi e degli odontoiatri della Provincia di Campobasso, riunitosi in modalità mista nella seduta del 12/01/2022, così costituito:

Nome e cognome	Carica	Presente	Assente
Giuseppe De Gregorio	Presidente	X	
Giulietta Terranova	Vice Presidente	X	
Michela Musacchio	Segretario	X	
Sergio Torrente	Tesoriere	X	
Biagio Apollonio	Componente	X*	
Giuseppe Cofelice	Componente		X
Domenico Coloccia	Componente (odont.)	X*	
Carolina De Vincenzo	Componente	X	
Laura Di Florio	Componente		X
Federico Di Renzo	Componente	X*	
Paola Di Rocco	Componente	X*	
Antonella Giordano	Componente	X	
Angelo Marcheggiani	Componente		X
Cesare Mariotti	Componente		X
Paolo Scarano	Componente	X	
Maria Grazia Terpolilli	Componente (odont.)	X*	
Giovina Vincelli	Componente	X*	

*: in collegamento telematico

prende in esame, per le determinazioni di competenza, l'argomento di cui in oggetto.

- VISTO il Regolamento UE 2016/679 (GDPR- *General Data Protection Regulation)* relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla

libera circolazione di tali dati, approvato dal Parlamento europeo e dal Consiglio dell'Unione europea in data 27.4.2016, che abroga la direttiva 95/46/CE e che mira a garantire una disciplina uniforme ed omogenea in tutto il territorio dell'Unione europea;

- CONSIDERATO che le norme introdotte dal Regolamento UE 2016/679 si traducono in obblighi organizzativi, documentali e tecnici che tutti i Titolari del trattamento dei dati personali devono osservare e far osservare;
- RITENUTO necessario ed opportuno stabilire modalità organizzative, misure procedimentali e regole di dettaglio, finalizzate anche ad omogeneizzare questioni interpretative, che permettano a questo Ente di poter agire con adeguata funzionalità ed efficacia nell'attuazione delle disposizioni introdotte dal nuovo Regolamento UE;
- VISTO lo schema di Regolamento allegato;
- VISTO il parere di regolarità tecnica del Data Protection Officer, Ing. Maurizio Giacci;

con votazione espressa all'unanimità dei presenti,

DELIBERA

di approvare il regolamento di cui all'oggetto, che si allega alla presente deliberazione per costituirne parte integrante.

IL SEGRETARIO
Dott.ssa Michela Musacchio

IL PRESIDENTE
Dott. Giuseppe De Gregorio

ORDINE DEI MEDICI CHIRURGHI E DEGLI ODONTOIATRI

PROVINCIA DI CAMPOBASSO

REGOLAMENTO PER LA TUTELA DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

Approvato dal Consiglio Direttivo nella seduta del 12/01/2022

TITOLO I

CAPO I

DISPOSIZIONI GENERALI

Oggetto

Al fine di garantire a ogni persona fisica il diritto alla protezione dei dati personali, l'Ordine dei Medici Chirurghi e degli Odontoiatri della Provincia di Campobasso, di seguito per brevità OMCeO CB, in attuazione del Regolamento Europeo del 27 aprile 2016 N. 679 (c.d. GDPR), adotta il presente regolamento che disciplina lo svolgimento dei trattamenti di dati personali eseguiti da questo Ordine.

L'OMCeO CB sostiene e promuove al suo interno ogni strumento di sensibilizzazione che possa consolidare il pieno rispetto del diritto alla protezione dei dati personali e migliorare la qualità del proprio operato.

Dal momento dell'assunzione del presente regolamento da parte dell'Ordine, lo stesso è messo a conoscenza di tutti i dipendenti che si impegnano a prenderne visione ed attenersi alle prescrizioni in esso contenute.

Definizioni

Ai fini del presente regolamento si intende per:

1) **archivio**: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

2) **consenso dell'interessato**: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

3) **dato personale**: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

4) **dati particolari**: categoria di dati personali che rivela l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;

5) **destinatario**: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

6) **limitazione di trattamento**: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

7) **profilazione**: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

8) **trattamento**: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

9) **violazione dei dati personali**: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Principi da applicare al trattamento dei dati personali

Tutte le attività di trattamento di dati personali operate dagli uffici dell'OMCeO CB dovranno osservare i seguenti principi:

a) liceità, correttezza e trasparenza: i dati personali devono essere trattati in modo lecito, corretto e trasparentenei confronti dell'interessato;

b) limitazione della finalità: i dati personali devono essere raccolti per finalità determinate, esplicite e legittime, esuccessivamente trattati in modo non incompatibile con tali finalità;

c) minimizzazione dei dati: i dati personali raccolti devono essere adeguati, pertinenti e limitati a quantonecessario rispetto alle finalità per le quali sono trattati;

d) esattezza: i dati personali raccolti devono essere esatti e, se necessario, aggiornati. Devono essere, inoltre,adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;

e) limitazione della conservazione: i dati personali raccolti devono essere conservati in una forma che consental'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;

f) integrità e riservatezza: i dati personali raccolti devono essere trattati in maniera da garantire un'adeguatasicurezza ivi compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti, dalla perdita, dalla distruzione e dal danno accidentale.

Con riferimento ai principi di limitazione della finalità, l'ulteriore trattamento dei dati personali ai fini dell'archiviazione nel pubblico interesse, per la ricerca scientifica o storica o ai fini statistici non è considerato incompatibile con le finalità iniziali.

Con riferimento al principio di limitazione della conservazione, i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente ai fini dell'archiviazione nel pubblico interesse, per la ricerca scientifica o storica o ai fini statistici.

Liceità del trattamento

Il trattamento dei dati è lecito senza il consenso dell'interessato se esso è necessario:

a) all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

b) per adempiere un obbligo legale al quale è soggetto il Titolare del Trattamento;

c) per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;

d) per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

e) per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

E' altresì lecito svolgere trattamenti di dati particolari qualora essi riguardano dati personali resi manifestamente pubblici dall'interessato o qualora essi:

a) sono necessari per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale;

b) sono necessari per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;

c) sono effettuati, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;

d) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;

e) sono necessari per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;

f) sono necessari per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità;

g) sono necessari per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale;

h) sono necessari a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato

Qualora il trattamento dei dati avvenga nella circostanza indicata al precedente punto h) il trattamento dovrà essere soggetto a garanzie adeguate per i diritti e le libertà dell'interessato. Tali garanzie dovranno assicurare che siano state predisposte misure tecniche e organizzative, in particolare quelle finalizzate a garantire il rispetto del principio della minimizzazione dei dati. Tali misure dovranno includere l'utilizzo della tecnica della pseudonimizzazione o di qualsiasi altra tecnica che non permetta più l'identificazione dell'interessato, qualora l'applicazione di tali misure non siano di ostacolo al conseguimento della finalità stabilita.

Qualora il trattamento dei dati non avvenga nell'ambito di alcuna circostanze rappresentate ai precedenti comma 1 e 2, esso è lecito solo se l'interessato ha prestato il proprio consenso.

Il consenso dovrà essere formulato attraverso la sottoscrizione di una dichiarazione scritta che dovrà essere conservata presso gli uffici dell' OMCeO CB al fine di dimostrare nel tempo il consenso prestato dall'interessato.

L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento su di esso basata prima della revoca.

CAPO II DIRITTI DELL'INTERESSATO

Diritti dell'interessato

Con riferimento ai dati personali trattati dall'OMCeO CB, l'interessato può avvalersi del:

a) **diritto di accesso**, ossia avere conferma dell'esistenza o meno di un trattamento di dati personali che lo riguardano e, in caso affermativo, di venire a conoscenza delle caratteristiche del trattamento;

b) **diritto di rettifica**, ossia richiedere la modifica di dati personali inesatti e/o l'integrazione di dati personali incompleti;

c) **diritto di cancellazione**, ossia richiedere l'immediata cancellazione dei dati personali se ne ricorrono i presupposti normativi;

d) **il diritto di limitazione**, ossia ottenere una limitazione al trattamento dei suoi dati personali;

e) **il diritto alla portabilità dei dati**, ossia ottenere, in caso di trattamenti effettuati con mezzi automatizzati, in formato strutturato i dati personali che lo riguardano al fine di trasferirli presso un'altra organizzazione;

f) **diritto di opposizione,** ossia di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, a trattamenti di dati personali che lo riguardano e svolti per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri oppure per il perseguimento del legittimo interesse del titolare del trattamento o di terzi.

a) **diritto di opposizione a processi decisionali automatizzati,** ossia richiedere di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.

Al fine di tutelare i propri diritti l'interessato può proporre reclamo all'Autorità Garante per la Protezione dei Dati Personali ovvero inviare una richiesta scritta al Titolare del Trattamento ovvero inviare una richiesta scritta al Responsabile per la Protezione dei Dati.

Informativa

Ai sensi dell'Art. 13 del GDPR è istituita un'area, all'interno del portale istituzionale dell'OMCeO CB e raggiungibile dalla pagina principale dello stesso, in cui saranno pubblicate le informative mediante le quali gli interessati potranno ottenere informazioni sui trattamenti di dati personali eseguiti dall'Ordine.

Per il tramite dell'informativa, che dovrà essere redatta in forma concisa, trasparente, intelligibile e con un linguaggio semplice e chiaro, l'interessato, qualora la raccolta dati avviene presso lo stesso, dovrà essere portato a conoscenza:

a) dell'identità e dei dati di contatto del titolare del trattamento;

b) dei dati di contatto del Responsabile della Protezione dei Dati;

c) delle finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;

d) dei legittimi interessi perseguiti dal Titolare del Trattamento o da terzi, qualora il trattamento si basi sulle circostanze indicate all'articolo 4, comma 1, lettera e);

e) degli eventuali destinatari o delle eventuali categorie di destinatari dei dati personali;

f) dell'eventualità che i dati personali vengano trasferiti a un paese terzo o a un'organizzazione internazionale;

g) del periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

h) dell'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;

i) qualora il trattamento sia basato sul consenso espresso dall'interessato, dell'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;

j) del diritto di proporre reclamo a un'autorità di controllo;

k) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;

l) dell'esistenza di un processo decisionale automatizzato, compresa la profilazione.

Per il tramite dell'informativa, che dovrà essere redatta in forma concisa, trasparente, intelligibile e con un linguaggio semplice e chiaro, l'interessato, qualora i dati non siano stati ottenuti presso lo stesso, dovrà essere portato a conoscenza:

a) dell'identità e dei dati di contatto del titolare del trattamento;

b) dei dati di contatto del Responsabile della Protezione dei Dati;

c) delle finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;

d) delle categorie di dati personali trattati;

e) degli eventuali destinatari o delle eventuali categorie di destinatari dei dati personali;

f) dell'eventualità che i dati personali vengano trasferiti a un paese terzo o a un'organizzazione internazionale;

g) del periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

h) dei legittimi interessi perseguiti dal Titolare del Trattamento o da terzi, qualora il trattamento si basi sulle circostanze indicate all'articolo 4, comma 1, lettera e);

i) dell'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;

j) qualora il trattamento sia basato sul consenso espresso dall'interessato, dell'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;

k) del diritto di proporre reclamo a un'autorità di controllo;

l) della fonte da cui hanno origine i dati personali e, se del caso, dell'eventualità che i dati provengano da fonti accessibili al pubblico;

m) dell'esistenza di un processo decisionale automatizzato, compresa la profilazione.

CAPO III TITOLARE DEL TRATTAMENTO, RESPONSABILE DEL TRATTAMENTO E RESPONSABILE DELLA PROTEZIONE DEI DATI

Titolare del trattamento

L'OMCeO CB è il Titolare del Trattamento dei dati personali raccolti presso i propri uffici e archiviati su supporti sia digitali che cartacei.

Il Titolare del Trattamento è responsabile del rispetto dei principi da applicare ai trattamenti di dati personali, con particolare riferimento alle misure tecniche e organizzative da porre in atto al fine di garantire i principi di integrità e riservatezza.

Tramite verifiche periodiche il Titolare del Trattamento vigila sulla osservanza, da parte dei designati e dei Responsabili del Trattamento, delle vigenti disposizioni in materia di trattamento dei dati, nonché delle misure tecniche e organizzative impartite attraverso il presente regolamento.

Responsabile del trattamento

Il Responsabile del Trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del Trattamento, ossia l'OMCeO CB.

Qualora l'affidamento di un servizio o la stipula di una convenzione preveda la presenza della figura del Responsabile del Trattamento dovranno essere individuati unicamente soggetti che presentino garanzie sufficienti per mettere in atto le misure tecniche e organizzative adeguate a soddisfare il rispetto dei principi di cui all'Art. 3 del presente regolamento e ogni disposizione stabilita della normativa vigente sulla protezione dei dati personali.

I rapporti tra il Titolare del Trattamento e i Responsabili del Trattamento dovranno essere stabiliti attraverso contratti o altri atti giuridici, stipulati in forma scritta.

Il contratto o altro atto giuridico dovrà identificare la materia disciplinata, la durata, la natura e la finalità, nonché il tipo di dati personali, le categorie di interessati e gli obblighi del Responsabile del Trattamento. In particolare, dovrà obbligare quest'ultimo:

a) a garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;

b) ad adottare le misure necessarie a garantire il trattamento in sicurezza di dati personali;

c) ad assistere il titolare del trattamento qualora quest'ultimo sia chiamato a dar seguito alle richieste per l'esercizio dei diritti dell'interessato;

d) a cancellare o restituire tutti i dati personali al termine della prestazione dei servizi e cancellare le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;

e) a porre a disposizione del Titolare del Trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi e contribuire alle attività di revisione, comprese le ispezioni, realizzati dal Titolare del

Trattamento o da un altro soggetto da questi incaricato;

f) a informare immediatamente il Titolare del Trattamento su ogni circostanza che, a suo parere, comporti la violazione del presente regolamento e di ogni altra disposizione in materia di protezione dei dati personali;

g) ad assistere il Titolare del Trattamento nelle procedure finalizzate alla valutazione degli impatti sulla protezione dei dati, fornendo allo stesso ogni informazione di cui è in possesso;

h) a informare il Titolare del Trattamento, senza ingiustificato ritardo, su avvenuti casi di violazione dei dati personali e assistere il Titolare del Trattamento nello svolgimento di ogni procedura conseguenziale, quale ad esempio la notifica di violazione all'Autorità Garante per la Protezione dei Dati Personali.

Responsabile della protezione dei dati

Ai sensi dell'Art. 37 del GDPR è istituita la figura del Responsabile della Protezione dei Dati (c.d. DPO o RPD) che è nominato dal Titolare del Trattamento.

Il Responsabile della Protezione dei Dati è la figura professionale incaricata dei seguenti compiti:

a) informare e fornire consulenza al Titolare del Trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR e dalle altre normative relative alla protezione dei dati. In tal senso il Responsabile della Protezione dei Dati può indicare al Titolare del Trattamento i settori funzionali ai quali riservare un audit interno o esterno in tema di protezione dei dati, le attività di formazione interna per il personale che tratta dati personali, e a quali trattamenti dedicare maggiori risorse e tempo in relazione al rischio riscontrato;

b) sorvegliare l'osservanza del GDPR e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità del Titolare del Trattamento;

c) fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento;

d) cooperare con l'Autorità Garante per la Protezione dei Dati Personali e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento.

La figura del Responsabile della Protezione dei Dati è incompatibile con chi determina le finalità o i mezzi del trattamento. In particolare, risulta con la stessa incompatibile la figura del responsabile del trattamento.

Il Responsabile della Protezione dei Dati opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti. In particolare, non deve ricevere istruzioni in merito al loro svolgimento né sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati.

Il Responsabile della Protezione dei Dati non può essere rimosso o penalizzato dal Titolare del Trattamento per l'adempimento dei propri compiti.

Ferma restando l'indipendenza nello svolgimento di detti compiti, il Responsabile della Protezione dei Dati riferisce direttamente al rappresentante legale pro tempore del Titolare del Trattamento o suo delegato.

Registro delle attività di trattamento

Ai sensi dell'Art. 30 del GDPR è istituito il Registro delle Attività di Trattamento che identifica tutti i trattamenti di dati personali operati dall' OMCeO CB.

Il Registro delle Attività di Trattamento dovrà riportare i dati di contatto dell'Ordine e del Responsabile della Protezione dei Dati, inoltre per ogni trattamento eseguito le seguenti informazioni:

a) le finalità del trattamento;

b) i dati di contatto di un eventuale contitolare del trattamento;

c) la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;

d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;

e) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;

f) ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

g) il richiamo alle misure di sicurezza tecniche e organizzative adottate.

Valutazione degli impatti sulla sicurezza

Ai sensi dell'art. 35 del GDPR l'OMCeO CB attuerà la valutazione degli impatti sulla sicurezza (c.d. PIA) per ogni trattamento che possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

Fermo restando quanto indicato dall'art. 35 del GDPR, verrà condotta una PIA nel caso in cui un trattamento ricada in almeno due delle seguenti circostanze:

a) trattamenti valutativi o di scoring, compresa la profilazione e attività predittive, concernenti aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato;

b) decisioni automatizzate che producono significativi effetti giuridici o di analoga natura, ossia trattamenti finalizzati ad assumere decisioni su interessati che producano effetti giuridici sulla persona fisica ovvero che incidono in modo analogo significativamente su dette persone fisiche;

c) monitoraggio sistematico, ossia trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di un'area accessibile al pubblico; d) trattamenti di dati particolari;

e) trattamenti di dati su larga scala;

f) combinazione o raffronto di insiemi di dati, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;

g) dati relativi a interessati vulnerabili, ossia ogni interessato particolarmente vulnerabile e meritevole di specifica tutela per il quale si possa identificare una situazione di disequilibrio nel rapporto con il Titolare del trattamento, come i dipendenti dell'Ordine, soggetti con patologie psichiatriche, richiedenti asilo, pazienti, anziani e minori;

h) utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;

i) tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

Qualora le risultanze di una PIA indicassero l'esistenza di un rischio residuale elevato, il trattamento oggetto di valutazione potrà essere eseguito solo dopo la consultazione con l'Autorità Garante per la Protezione dei Dati Personali.

Il Titolare del Trattamento consulta l'Autorità Garante per la Protezione dei Dati Personali anche nei casi in cui la vigente legislazione stabilisce l'obbligo di consultare e/o ottenere la previa autorizzazione della medesima

autorità, per trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale e alla sanità pubblica.

La documentazione prodotta a seguito di una PIA sarà tenuta in formato digitale, acquisita al protocollo e posta in conservazione sostitutiva.

Il Responsabile della Protezione dei Dati sovrintende all'esecuzione di una PIA e segnala al Titolare del Trattamento l'insorgere di ogni eventuale problematica che ne possa ostacolare la corretta gestione

TITOLO II
MISURE TECNICHE ED ORGANIZZATIVE PER LA PROTEZIONE DA TRATTAMENTI NON AUTORIZZATI O ILLECITI, DALLA PERDITA, DALLA DISTRUZIONE E DAL DANNO ACCIDENTALE

CAPO I
MISURE ORGANIZZATIVE

Linee guida generali

Il trattamento di dati personali dovrà essere eseguito soltanto :

a) per lo svolgimento delle funzioni istituzionali, nei limiti stabiliti dalla legge e dai regolamenti attualmente in vigore nei singoli uffici;

b) per esigenze di tipo operativo e gestionale;

c) per ottemperare ad obblighi di legge;

d) per finalità di programmazione operativa;

e) per dare esecuzione ad un servizio o ad una o più operazioni concorsualmente convenute.

Nell'esecuzione di un trattamento dovranno essere raccolti i soli dati personali necessari al raggiungimento della specifica finalità.

Le informazioni trattate dagli uffici dell'OMCeO CB dovranno essere opportunamente cancellate o distrutte nei casi in cui:

a) non siano più utili al raggiungimento delle finalità istituzionali;

b) siano relative alla cessazione per qualsiasi causa di trattamenti di dati personali non più necessari o siano eccedenti rispetto alle finalità per le quali sono stati raccolti o successivamente trattati;

c) gli scopi per le quali sono state raccolte e trattate non siano più determinati, espliciti e legittimi oppure siano diventate incompatibili con tali scopi;

d) risultino scaduti i termini legittimi di conservazione anche con riferimento al tempo necessario agli scopi per i quali sono stati raccolti o successivamente trattati, siano essi determinati da norme di legge generali e/o di settore (ad es. dieci anni per la conservazione delle scritture contabili) oppure dalle finalità per le quali i dati sono stati raccolti o in relazione alle quali devono essere conservati (ad es. contenziosi);

e) l'interessato ne richieda la cancellazione nell'esercizio dei propri diritti di cui all'Art. 4 del presente regolamento.

Il Responsabile della Protezione dei Dati, di cui all'Art. 7 del presente regolamento, dovrà essere tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. A tal fine:

a) il Responsabile della Protezione dei Dati dovrà essere invitato a partecipare alle riunioni di coordinamento dei Dirigenti/Responsabili P.O. che abbiano per oggetto questioni inerenti il trattamento di dati personali;

b) il Responsabile della Protezione dei Dati deve disporre tempestivamente di tutte le informazioni pertinenti sulle decisioni che impattano sulla protezione dei dati, in modo da poter rendere una consulenza idonea.

Al Responsabile della Protezione dei Dati dovrà essere fornito il supporto necessario per assolvere ai compiti attribuiti e per accedere ai dati personali e ai trattamenti. In particolare viene assicurato il supporto attivo per lo svolgimento dei compiti da parte dei Dirigenti/Responsabili P.O. e degli organi collegiali, nonché l'accesso ai settori funzionali dell'OMCeO CB.

Comunicazione dei dati personali

La comunicazione e la diffusione dei dati personali trattati dall' OMCeO CB a soggetti pubblici, privati oppure a enti pubblici economici sono ammesse in presenza di specifiche previsioni di legge o di regolamento.

Ad eccezione delle ipotesi di trasferimento di dati tra enti pubblici o necessari per indagini di Pubblica Sicurezza è esclusa la messa a disposizione o la consultazione di dati in blocco o la ricerca per nominativo di tutte le informazioni contenute nelle banche dati, senza limiti di procedimento o di settore.

Sono escluse dalla previsioni del precedente comma 2 le liste elettorali.

Soggetti designati al trattamento

Sono soggetti designati al trattamento i Dirigenti/Responsabili P.O. e in quanto tali sono autorizzati a eseguire, per conto dell' OMCeO CB, le attività di trattamento di dati personali necessarie allo svolgimento dei procedimenti propri dell'ufficio di competenza.

I Dirigenti/Responsabili P.O. sovrintendono, altresì, a che i trattamenti di dati personali, che saranno svolti all'interno del proprio ufficio di competenza, avvengano nel rispetto delle disposizioni del presente regolamento.

I Dirigenti/Responsabili P.O. hanno facoltà di nominare, tra i soggetti che operano alle dipendenze dell'OMCeO CB, ulteriori designati al trattamento, ossia ulteriori soggetti che nel proprio ufficio di competenza sono autorizzati a svolgere attività di trattamento dei dati personali. La designazione deve essere formulata compatibilmente alle mansioni assegnate al dipendente e fornendo a quest'ultimo opportune istruzioni scritte.

I soggetti designati al trattamento devono garantire la massima riservatezza, nonché il rispetto delle disposizioni del presente regolamento e in particolare l'applicazione dei principi di cui all'art. 3 del presente regolamento e dei diritti dell'interessato di cui all'art. 4 del presente regolamento.

I soggetti che trattano dati personali per conto dell'OMCeO CB rispondono per i danni cagionati al patrimonio e alla reputazione di questo Ordine a seguito della violazione delle disposizioni contenute sia nel presente regolamento che nella vigente normativa in materia di tutela dei dati personali.

Tenuta del Registro delle Attività di Trattamento

I Dirigenti/Responsabili P.O, relativamente ai trattamenti svolti nei propri uffici di competenza, redigono il Registro delle Attività di Trattamento, di cui all'Art. 8 del presente regolamento, e lo aggiornano ogni qual volta si renda necessario dar luogo a un nuovo trattamento di dati personali.

Il Registro della Attività di Trattamento dovrà essere soggetto al processo di revisione annuale durante il quale i Dirigenti/Responsabili P.O dovranno operare una verifica dei contenuti con particolare riferimento a eventuali dismissioni di trattamenti di dati personali o evoluzioni delle misure tecnico organizzative implementate.

Il Responsabile della Protezione dei Dati sovrintende al processo di iniziale stesura, successivi aggiornamenti e revisioni del Registro delle Attività di Trattamento e segnala al Titolare del Trattamento l'insorgere di ogni eventuale problematica che ne possa ostacolare la corretta gestione.

Il Titolare del Trattamento trasmette al Responsabile della Protezione dei Dati il Registro delle Attività dei Trattamenti che viene formato:

a) al termine del processo di iniziale stesura;

b) qualora si determini un nuovo aggiornamento;

c) al termine del processo di revisione annuale.

Il Registro delle Attività di Trattamento è tenuto in formato digitale, è acquisito al protocollo e posto in conservazione sostitutiva.

Tenuta delle Informative

I Dirigenti/Responsabili P.O, relativamente ai trattamenti svolti nei propri uffici di competenza, redigono le informative di cui all'Art. 10 del presente regolamento, e apportano le necessarie rettifiche ogni qual volta il corrispondente trattamento di dati personali subisce una modifica nelle sue caratteristiche principali.

1. I Dirigenti/Responsabili P.O sovrintendono, altresì, alla pubblicazione delle stesse nella corrispondente sezione istituita all'interno del portale istituzionale dell'OMCeO CB.

Il Responsabile della Protezione dei Dati sovrintende alla tenuta delle informative redatte dall' OMCeO CB e segnala al Titolare del Trattamento l'insorgere di ogni eventuale problematica che ne possa ostacolare la corretta gestione.

Rapporti con i Responsabili del Trattamento

Qualora l'affidamento di un servizio o la stipula di una convenzione preveda la presenza della figura del Responsabile del Trattamento, di cui all'Art. 6 del presente regolamento, ossia di un soggetto terzo che esegue un trattamento di dati per conto dell' OMCeO CB, è compito dei Dirigenti/Responsabili P.O. ovvero di chiunque altro soggetto che per conto di questo Ordine ha facoltà di determinare l'affidamento o stipulare la convenzione, di individuare unicamente soggetti economici che presentino garanzie sufficienti per mettere in atto le misure tecniche e organizzative adeguate a soddisfare il rispetto dei principi di cui all'Art. 3 del presente regolamento e ogni disposizione stabilita dalla normativa vigente sulla protezione dei dati personali.

E' compito altresì dei Dirigenti/Responsabili P.O. ovvero di chiunque altro soggetto che per conto di questo Ordine ha facoltà di determinare l'affidamento o stipulare la convenzione di disciplinare i rapporti con i Responsabili del Trattamento attraverso contratti o altri atti giuridici così come indicato ai punti 3 e 4 dell'Art. 6 del presente regolamento.

Registri di inventario dei dispositivi tecnologici e dei software autorizzati

Ai sensi di quanto disposto dall'Agenzia per l'Italia Digitale attraverso la circolare N. 2/2017, sono istituiti il registro di inventario dei dispositivi tecnologici e il registro dei software autorizzati.

Il registro di inventario dei dispositivi tecnologici dovrà indicare tutte le risorse hardware attive operanti all'interno della struttura informatica dell'OMCeO CB e per ognuna di essa riportare le seguenti informazioni:

a) Denominazione del dispositivo;
b) Funzione del sistema;
c) Numero seriale;
d) Indirizzo IP assegnato;
e) Ufficio assegnato.

Il registro dei software autorizzati dovrà indicare i software autorizzati a operare all'interno della struttura informatica dell'OMCeO CB e per ognuno di essi riportare:

a) la denominazione del software;
b) la casa produttrice;
c) la versione del software.

Tenuta del registri dell'inventario dei dispositivi tecnologici e dei software autorizzati

I registri di inventario dei dispositivi tecnologici attivi e dei software autorizzati di cui al precedente articolo sono tenuti dal soggetto a cui fa capo la responsabilità dei sistemi informativi, il quale dovrà provvedere all'iniziale stesura e ai successivi aggiornamenti, che dovranno aver luogo ogni qual volta nuovi dispositivi vengono introdotti nel sistema informatico e ogni qual volta si ha la necessità di adottare nuovi software necessari allo svolgimento delle funzioni istituzionali.

Il soggetto a cui fa capo la responsabilità dei sistemi informativi dovrà eseguire annualmente una verifica di corrispondenza tra i contenuti dei due registri e i dispositivi tecnologici attivi e i software effettivamente operanti all'interno della struttura informatica dell' OMCeO CB.

Violazione dei dati personali

I designati al trattamento dei dati personali e i Responsabili del Trattamento dovranno notificare al Titolare del Trattamento e al Responsabile per la Protezione dei Dati il verificarsi di ogni evento di violazione dei dati personali trattati dall'OMCeO CB ossia il verificarsi di eventi che causano trattamenti non autorizzati o illeciti, perdita, distruzione e danno accidentale dei dati.

Al verificarsi di ogni evento di violazione, il Titolare del Trattamento, previa consultazione del Responsabile per la Protezione dei Dati, provvederà a notificare l'accaduto all'Autorità Garante per la Protezione dei Dati Personali qualora si ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati quali:

a) danni fisici, materiali o immateriali alle persone fisiche;
b) perdita del controllo dei dati personali;
c) limitazione dei diritti, discriminazione;
d) furto o usurpazione d'identità;
e) perdite finanziarie, danno economico o sociale.
f) corruzione del sistema di anonimizzazione dei dati;
g) pregiudizio alla reputazione;
h) perdita di riservatezza dei dati personali protetti da segreto professionale.

La notifica, di cui al precedente comma, avverrà entro le 72 ore dal momento in cui il Titolare del Trattamento è venuto a conoscenza dell'evento di violazione.

Se il rischio per i diritti e le libertà degli interessati coinvolti dall'evento di violazione di dati personali è elevato, allora questi ultimi saranno informati, senza ingiustificato ritardo, circa la natura della violazione verificatasi.

I rischi per i diritti e le libertà degli interessati saranno considerati "elevati" quando la violazione può:

a) coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
b) riguardare categorie particolari di dati personali;
c) comprendere dati che possono accrescere ulteriormente i potenziali rischi (dati di localizzazione, finanziari, relativi alle abitudini e preferenze, etc.);
d) comportare rischi imminenti e con un'elevata probabilità di accadimento (rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito, etc.);
e) impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (utenti deboli, minori, soggetti indagati, etc.).

Gli eventi di violazione dei dati personali trattati dall'OMCeO CB saranno documentate all'interno del Registro degli Eventi di Data Breach, che, oltre ai riferimenti temporali legati all'accaduto, riporta le circostanze a esso relative, le conseguenze e i provvedimenti adottati.

Il Registro degli Eventi di Data Breach sarà tenuto in formato digitale, acquisito al protocollo e posto in conservazione sostitutiva.

CAPO II MISURE TECNICHE

Trattamenti disgiunto dei dati particolari

Il trattamento dei dati particolari sono soggetti a gestione disgiunta, ossia:

a) l'insieme dei dati personali che identificano una persona dovrà essere trattato separatamente dall'insieme dei dati particolari a essa collegati;

b) il collegamento tra le due tipologie di insiemi avviene attraverso l'utilizzo di codici identificativi atti a impedire l'immediata riconducibilità.

L'adozione di tecniche di criptazione, che rendono l'intero insieme dei dati particolari non comprensibili/intelligibili a persone non autorizzate, sostituisce l'obbligo del trattamento disgiunto di cui al precedente punto.

Le regole di cui ai precedenti punti sono applicate a ogni trattamento di dati particolari, sia che esso avvenga su supporto cartaceo che digitalmente.

Trattamenti eseguiti mediante l'utilizzo dei documenti in formato cartaceo

I documenti in formato cartaceo che contengono dati personali dovranno essere conservati in archivi ciechi e dotati di serratura.

I documenti in formato cartaceo che contengono dati personali dovranno essere consultati solo all'interno degli uffici dell'Ordine non accessibili al pubblico. In caso di allontanamento, anche temporaneo, dalla postazione di lavoro dovranno essere poste in essere tutte le misure necessarie a evitare che soggetti non autorizzati possano accedere ai dati personali contenuti nei documenti in consultazione.

Le attività di stampa, fotocopia o acquisizione ottica di documenti contenenti dati personali dovranno essere svolte nel rispetto del principio di riservatezza, ossia evitando che soggetti non autorizzati possano visualizzare il contenuto dei documenti oggetto di trattamento. Al termine dell'attività il documento oggetto di trattamento dovrà essere rimosso dai dispositivi di stampa, fotocopia o acquisizione ottica.

Gestione dei dispositivi tecnologici e dei software

E' fatto divieto di installare qualsiasi software, soggetto a tutela autoriale, contenuto in dischetti, DVD-ROM e altri dispositivi removibili, o direttamente scaricato da Internet, senza la "licenza d'uso" o senza autorizzazione del Titolare del Trattamento.

E' fatto divieto di utilizzare gli strumenti forniti in dotazione, nelle componenti sia hardware che software, in modo improprio o per fini personali.

All'interno della struttura informatica dell'OMCeO CB è consentito esclusivamente l'utilizzo di dispositivi tecnologici e software autorizzati, ossia dei dispositivi tecnologici e dei software elencati nei registri di inventario di cui all'Art. 17 del presente regolamento.

Il soggetto a cui fa capo la responsabilità dei sistemi informativi provvede alla rimozione dei dispositivi non autorizzati e dei software non autorizzati o comunque non necessari allo svolgimento delle funzioni istituzionali.

Controllo degli accessi ai dispositivi e ai software

L'accesso alle postazioni di lavoro, alle unità server, ai dispositivi di rete configurabili e ai software dovrà avvenire attraverso l'utilizzo di sistemi di identificazione, autenticazione e autorizzazione del soggetto che opera su di essi.

Qualora sia adottata la password come elemento di autenticazione essa dovrà:

a) avere una lunghezza non inferiore a 8 caratteri oppure, nel caso in cui il sistema non lo dovesse prevedere, di lunghezza pari al massimo consentito;

b) essere cambiata almeno ogni 6 mesi;

c) contenere, ove possibile, almeno un numero e un carattere speciale;

d) essere diversa dalle almeno ultime due precedentemente utilizzate;

e) non contenere riferimenti che permettano un agevole riconducibilità all'utente o ad ambiti noti;

f) non essere memorizzata in funzioni di log-in automatico, in un tasto funzionale o nel browser utilizzato per la navigazione internet.

E' vietato divulgare ad altri le credenziali personali di accesso. Il titolare delle credenziali è responsabile di tutte le azioni e le funzioni svolte per il tramite delle sue credenziali. A tal fine egli in caso di allontanamento, anche temporaneo, dalla postazione di lavoro dovrà attivare la funzionalità di blocco dell'elaboratore quali ad esempio la digitazione in contemporanea dei tasti CTRL+ALT+CANC.

Le utenze dotate di privilegi di amministrazione di una postazione di lavoro o di una unità server sono utilizzate esclusivamente per dar luogo ad attività di gestione straordinaria delle componenti hardware e software. L'utilizzo ordinario di una postazione di lavoro o di una unità server deve essere effettuato mediante l'accesso con utenze dotate di privilegi limitati.

Le utenze dotate di privilegi di amministrazione definite per ogni postazione di lavoro, unità server, dispositivi di rete configurabili e software dovranno essere riportate nel registro delle password che sarà custodito dal responsabile del sistema informativo.

Gestione delle postazioni di lavoro e delle unità server

E' vietato, all'interno della struttura informatica dell'OMCeO CB, l'utilizzo di postazioni di lavoro e unità server non dotati di software atti a rilevare la presenza e bloccare l'esecuzione di malware (c.d. antivirus). Detti software dovranno essere aggiornabili, nella conoscenza delle impronte virali, in maniera automatico.

E' vietato, all'interno della struttura informatica dell'OMCeO CB, l'utilizzo di postazioni di lavoro e unità server su cui operano sistemi operativi non aggiornati o non più aggiornabili. Laddove applicabile l'aggiornamento dei sistemi operativi dovrà essere eseguito in maniera automatico.

Il soggetto a cui fa capo la responsabilità dei sistemi informativi verifica trimestralmente la necessità di operare sui dispositivi di rete l'aggiornamento firmware, procedendo in tal senso quando necessario. Esegue altresì la medesima operazione di verifica con la medesima periodicità per ogni postazioni di lavoro e unità server su cui operano sistemi operativi non aggiornabili in maniera automatica.

In caso di malfunzionamento dell'elaboratore in uso, che possa far sospettare la presenza di un virus, è fatto obbligo di:

a) sospendere ogni operazione;

b) contattare immediatamente il soggetto a cui fa capo la responsabilità dei sistemi informativi;

c) chiudere il sistema e le relative applicazioni.

La copia dei dati personali trattati dall'OMCeO CB su supporti di memorizzazione di massa esterni è consentita solo se necessaria per lo svolgimento delle funzioni istituzionali. In tal caso dovranno essere adottati sistemi per la criptazione dei dati affinché questi siano resi non comprensibili/intelligibili a persone non autorizzate.

Qualora venga meno la possibilità di adottare i sistemi per la criptazione dei dati di cui al comma precedente, i supporti di memorizzazione di massa esterni che contengono dati personali non potranno lasciare la sede ospitante gli uffici, dovranno essere utilizzati esclusivamente all'interno di quest'ultima e dovranno essere custoditi con diligenza e conservati in armadi o contenitori muniti di serratura.

Comunicazioni mediante rete

L'utilizzo della rete Internet e dei servizi accessibili per il suo tramite è consentito solo se necessario per lo svolgimento delle funzioni istituzionali. Sono vietati comportamenti che possano arrecare danno alla reputazione e al patrimonio dell'OMCeO CB.

Il trattamento dei dati personali attraverso la rete Internet dovrà aver luogo solo attraverso l'utilizzo di comunicazioni non in chiaro, ossia comunicazioni che adottano, nello scambio dei dati, i protocolli crittografici.

L'accesso alla infrastruttura dell'OMCeO CB mediante tecnologia wireless èconsentita solo se necessaria per lo svolgimento delle funzioni istituzionali. In tal caso dovranno essere adottati sistemi di identificazione e autorizzazione dei terminali mediante tecniche di filtraggio del MAC ovvero sistemi di identificazione, autenticazione e autorizzazione dell'utente.

Le attività di accesso da remoto alle postazioni di lavoro, alle unità server e ai dispositivi di rete sono consentite solo se eseguite mediante l'utilizzo di connessioni protette e sotto il controllo e il monitoraggio del soggetto a cui fa capo la responsabilità dei sistemi informativi.

Utilizzo del servizio di posta elettronica

L'utilizzo della posta elettronica è consentito solo se necessario per lo svolgimento delle funzioni istituzionali. Sono vietati comportamenti che possano arrecare danno alla reputazione e al patrimonio dell'OMCeO CB.

L'account di posta elettronica è uno strumento di proprietà dell'OMCeO CB ed è conferito in uso per l'esclusivo svolgimento delle mansioni lavorative affidate.

Ad uno stesso soggetto possono essere assegnate più caselle di posta elettronica, che possono anche essere condivise con altri utenti dello stesso ufficio.

Attraverso le caselle gli utenti rappresentano pubblicamente l'OMCeO CB e per questo è fatto obbligo di utilizzare la posta elettronica in modo lecito, professionale e comunque tale da riflettere positivamente l'immagine dell'Ordine.

Gli utenti sono responsabili del corretto utilizzo delle caselle di posta elettronica affidata e devono:

- conservare la password nella massima riservatezza e con la massima diligenza;
- mantenere la casella in ordine, cancellando documenti inutili e allegati ingombranti;
- prestare ai contenuti della corrispondenza ricevuta e non aprire allegati o selezionare hyperlink testuali contenuti in e-mail di dubbia provenienza o ricevute nell'ambito di un contesto avulso da quello lavorativo. In tali casi dovranno non aprire il messaggio e segnalare immediatamente l'accaduto al responsabile del sistema informativo;
- rispondere alle e-mail pervenute solo da mittenti conosciuti.

Non è consentito l'invio automatico della posta ricevuta su account istituzionale verso un indirizzo di e-mail privato anche durante i periodi di assenza.

In caso di assenza improvvisa o prolungata ovvero per imprescindibili esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio ovvero per motivi di sicurezza del sistema informatico, il Titolare del Trattamento, per il tramite del soggetto a cui fa capo la responsabilità dei sistemi informativi, potrà accedere all'account di posta elettronica, prendendo visione dei messaggi, salvando o cancellando file. Di tale attività sarà redatto apposito verbale e informato il soggetto interessato alla prima occasione utile.

In caso di interruzione del rapporto di lavoro, l'indirizzo di posta elettronica verrà disabilitato entro un periodo massimo di 30 (trenta) giorni da quella data ed entro 90 (novanta) giorni si disporrà la definitiva e totale cancellazione dello stesso. In ogni caso, l'Ordine si riserva il diritto di conservare i messaggi di posta elettronica ritenuti rilevanti per le proprie finalità istituzionali.

Salvo l'utilizzo di appositi strumenti di cifratura i sistemi di posta elettronica non possono garantire la riservatezza delle informazioni trasmesse. Pertanto è fatto obbligo di valutare con attenzione l'invio di informazioni contenenti dati personali che potranno essere trasmessi se:

a) il destinatario è certo;

b) il destinatario è autorizzato a entrare in possesso dei dati personali.

Fermo restando l'applicazione di quanto disposto al precedente punto, è fatto, altresì, obbligo di adottare sistemi per la cifratura dei contenuti qualora le informazioni trasmesse attraverso la posta elettronica contengano dati particolari.

Procedure di backup dei dati

Sono adottate procedure volte a eseguire le copie di backup dei dati contenuti all'interno delle unità server e all'interno delle singole postazioni di lavoro.

Le procedure di backup dovranno essere eseguite quotidianamente, mediante l'utilizzo di procedure/software che ne garantiscono l'automatizzazione.

Il responsabile del sistema informativo sovrintende sulla corretta esecuzione delle procedure di backup e in particolare verifica semestralmente il corretto funzionamento delle procedure di recovery.

Distruzione dei dati

I supporti di memorizzazione di massa (hard disk, DVD, CD, etc.) destinati allo smaltimento dovranno essere oggetto di preventiva distruzione fisica attraverso sistemi di punzonatura, deformazione meccanica o apertura dell'involucro protettivo con danneggiamento delle superfici atte alla memorizzazione.

I supporti di memorizzazione di massa destinati al reimpiego dovranno essere oggetto di preventiva cancellazione dei dati che dovrà avvenire mediante l'utilizzo di software di wiping.

CAPO III VIOLAZIONI E RESPONSABILITÀ E DISPOSIZIONI FINALI

Responsabilità' in caso di violazione delle disposizioni in materia di privacy

Il mancato rispetto delle disposizioni previste dal presente Regolamento comporta la violazione degli obblighi previsti dalla normativa sulla protezione dei dati personali ed espone il Titolare del Trattamento a rischi sul piano delle responsabilità e delle sanzioni a livello civile, amministrativo e, nei casi più gravi, anche penale.

La violazione delle disposizioni previste dal presente regolamento e dalla normativa sulla protezione dei dati personali da parte dei soggetti designati al trattamento dei dati per conto dell'OMCeO CB rende possibile contestare il fatto e infliggere i relativi provvedimenti disciplinari previsti dal C.C.N.L. applicato, nonché a fronte di danni economici, la richiesta del conseguente risarcimento.

Rinvio

Per quanto non previsto nel presente regolamento, si applicano le disposizioni stabilite dalla normativa in materia di tutela delle persone fisiche con riguardo alla protezione dei dati personali, con particolare riferimento alle previsioni contenute nel Regolamento Europeo 2016/679 e nel Codice della Privacy vigente in funzione delle modifiche e integrazioni operate dal D.Lgs. 101/2018.

Il presente regolamento sarà aggiornato a seguito di ulteriori modifiche alla vigente normativa in materia di tutela delle persone fisiche con riguardo alla protezione dei dati personali.

Entrata in vigore del regolamento e forme di pubblicità

Il presente Regolamento, approvato dal Consiglio Direttivo dell'Ordine dei Medici Chirurghi e degli Odontoiatri della provincia di Campobasso, nella seduta del 12/01/2022 con delibera N. 32, è approvato dal Comitato Centrale della FNOMCeO e trasmesso alla Federazione al Ministero della Salute che, ai sensi dell'art. 35 del D.P.R. 5 aprile 1950, n. 221, nel termine di tre mesi può, con decreto motivato, disporre l'annullamento per motivi di legittimità. Il presente Regolamento è reso pubblico mediante inserimento sul sito istituzionale dell'OMCeO di Campobasso ed entra in vigore il quindicesimo giorno successivo alla sua pubblicazione.

ORDINE PROVINCIALE DEI MEDICI-CHIRUGHI E DEGLI ODONTOIATRI DELLA PROVINCIA DI CAMPOBASSO

Via Mazzini, 129/A - Campobasso (CB)

PEC:info.cb@pec.omceo.it

TELEFONO: 0874.69177

REGISTRO DELLE ATTIVITA' DI TRATTAMENTO

ESEGUITE NEL RUOLO DI

RESPONSABILE DEL TRATTAMENTO

Riferimenti e versione

Data del documento: 04-09-2023

Versione del documento: B

Stato del documento: definitivo

1. Identificazione e dati di contatto del Responsabile del Trattamento

Il responsabile del trattamento dei dati è Ordine Provinciale dei Medici-Chirughi e degli Odontoiatri della Provincia di Campobasso. I dati di contatto del responsabile sono quelli riportati nella prima pagina del presente documento.

2. Identificazione e dati di contatto del Responsabile della protezione dei dati

Il Responsabile della protezione dei dati designato ai sensi dell’art. 37 del Regolamento UE 2016/679 è il Dott. Ing. Maurizio GIACCI che può essere contattato alla casella di posta elettronica certificata maurizio.giacci@ingpec.eu

3. Prospetto riassuntivo

TITOLARE DEL TRATTAMENTO	DENOMINAZIONE
FONDAZIONE ENPAM	ASSISTENZA DOMICILIARE
FONDAZIONE ENPAM	COMMISSIONE MEDICA PROVINCIALE
FONDAZIONE ENPAM	DOMANDA DI PENSIONE ORDINARIA, DI PENSIONE PER ...
FONDAZIONE ENPAM	OSPITALITA' IN CASE DI RIPOSO
FONDAZIONE ENPAM	SUSSIDI STRAORDINARI UNA TANTUM
FONDAZIONE ENPAM	SUSSIDIO AGGIUNTIVO
FONDAZIONE ENPAM	SUSSIDIO PER CALAMITA' NATURALI
FONDAZIONE ENPAM	SUSSIDIO SOSTITUTIVO DEL REDDITO

4. Elenco dei trattamenti

4.1 Assistenza domiciliare

(Fondazione Enpam)

4.1.1 Titolare del trattamento

Denominazione: Fondazione Enpam

Rappresentante: Presidente

DPO: Dott. Giorgio Boni - Piazza Vittorio Emanuele II, n.78 – 00185 Roma - PEC dpo@pec.enpam.it

4.1.2 Descrizione

Gestione amministrativa delle richieste di accesso al servizio di assistenza domiciliare erogato dalla Fondazione Enpam a favore degli iscritti dell'Ordine. In tale ambito, l'ordine raccoglie la documentazione inerente la richiesta, convoca il richiedente per la visita medica da parte della Commissione Provinciale Enpam, redige il verbale di visita e invia il fascicolo alla Fondazione Enpam.

4.1.3 Uffici che trattano i dati

Nessun ufficio specificato

4.1.4 Responsabili del trattamento

Società affidataria del servizio di conservazione digitale sostitutiva
Società affidatarie del servizio di manutenzione dei software di ufficio
Società affidatarie del servizio di manutenzione dell'hardware

4.1.5 Soggetti destinatari

Fondazione Enpam

4.1.6 Trasferimenti di dati verso un paese terzo

Il trattamento non è soggetto ad alcun trasferimento di dati verso un paese terzo

4.1.7 Termini previsti per la cancellazione delle diverse categorie di dati

I dati forniti verranno conservati per il tempo necessario al conseguimento delle finalità per le quali sono stati raccolti o per un periodo ulteriore se così disposto dalle norme di diritto, nonché dalle normative in materia di tenuta della documentazione amministrativa o qualora si renda necessario proseguire nell'archiviazione ai fini del pubblico interesse

4.1.8 Ubicazione degli archivi

I dati in formato digitale sono memorizzati all'interno delle postazioni di lavoro assegnate agli uffici e nel server dell'Ente. I dati in formato cartaceo sono custoditi in armadi dotati di serratura

4.2 Commissione medica provinciale

(Fondazione Enpam)

4.2.1 Titolare del trattamento

Denominazione: Fondazione Enpam

Rappresentante: Presidente

DPO: Dott. Giorgio Boni - Piazza Vittorio Emanuele II, n.78 – 00185 Roma - PEC dpo@pec.enpam.it

4.2.2 Descrizione

Gestione amministrativa delle attività svolte dai componenti della Commissione medica, nominata ai sensi dell'Art. 21 del Regolamento Fondo di Previdenza Generale, per gli accertamenti finalizzati al riconoscimento della pensione per inabilità.

4.2.3 Uffici che trattano i dati

Nessun ufficio specificato

4.2.4 Responsabili del trattamento

Società affidataria del servizio di conservazione digitale sostitutiva
Società affidatarie del servizio di manutenzione dei software di ufficio
Società affidatarie del servizio di manutenzione dell'hardware

4.2.5 Soggetti destinatari

Fondazione Enpam

4.2.6 Trasferimenti di dati verso un paese terzo

Il trattamento non è soggetto ad alcun trasferimento di dati verso un paese terzo

4.2.7 Termini previsti per la cancellazione delle diverse categorie di dati

I dati forniti verranno conservati per il tempo necessario al conseguimento delle finalità per le quali sono stati raccolti o per un periodo ulteriore se così disposto dalle norme di diritto, nonché dalle normative in materia di tenuta della documentazione amministrativa o qualora si renda necessario proseguire nell'archiviazione ai fini del pubblico interesse

4.2.8 Ubicazione degli archivi

I dati in formato digitale sono memorizzati all'interno delle postazioni di lavoro assegnate agli uffici e nel server dell'Ente. I dati in formato cartaceo sono custoditi in armadi dotati di serratura

4.3 Domanda di pensione ordinaria, di pensione per invaliditÃ , di pensione indiretta o di reversibilitÃ

(Fondazione Enpam)

4.3.1 Titolare del trattamento

Denominazione: Fondazione Enpam

Rappresentante: Presidente

DPO: Dott. Giorgio Boni - Piazza Vittorio Emanuele II, n.78 – 00185 Roma - PEC dpo@pec.enpam.it

4.3.2 Descrizione

Gestione amministrativa delle domande di pensione erogate dalla Fondazione Enpam a favore degli iscritti dell'Ordine. In tale ambito, l'ordine raccoglie la documentazione inerente la richiesta e la trasmette alla Fondazione Enpam

4.3.3 Uffici che trattano i dati

Nessun ufficio specificato

4.3.4 Responsabili del trattamento

Società affidataria del servizio di conservazione digitale sostitutiva
Società affidatarie del servizio di manutenzione dei software di ufficio
Società affidatarie del servizio di manutenzione dell'hardware

4.3.5 Soggetti destinatari

Fondazione Enpam

4.3.6 Trasferimenti di dati verso un paese terzo

Il trattamento non è soggetto ad alcun trasferimento di dati verso un paese terzo

4.3.7 Termini previsti per la cancellazione delle diverse categorie di dati

I dati forniti verranno conservati per il tempo necessario al conseguimento delle finalità per le quali sono stati raccolti o per un periodo ulteriore se così disposto dalle norme di diritto, nonché dalle normative in materia di tenuta della documentazione amministrativa o qualora si renda necessario proseguire nell'archiviazione ai fini del pubblico interesse

4.3.8 Ubicazione degli archivi

I dati in formato digitale sono memorizzati all'interno delle postazioni di lavoro assegnate agli uffici e nel server dell'Ente. I dati in formato cartaceo sono custoditi in armadi dotati di serratura

4.4 Ospitalita' in case di riposo

(Fondazione Enpam)

4.4.1 Titolare del trattamento

Denominazione: Fondazione Enpam

Rappresentante: Presidente

DPO: Dott. Giorgio Boni - Piazza Vittorio Emanuele II, n.78 – 00185 Roma - PEC dpo@pec.enpam.it

4.4.2 Descrizione

Gestione amministrativa delle richieste di accesso al servizio di ospitalità nelle case di riposo erogato dalla Fondazione Enpam a favore degli iscritti dell'Ordine. In tale ambito, l'ordine raccoglie la documentazione inerente la richiesta e la invia alla Fondazione Enpam

4.4.3 Uffici che trattano i dati

Nessun ufficio specificato

4.4.4 Responsabili del trattamento

Società affidataria del servizio di conservazione digitale sostitutiva
Società affidatarie del servizio di manutenzione dei software di ufficio
Società affidatarie del servizio di manutenzione dell'hardware

4.4.5 Soggetti destinatari

Fondazione Enpam

4.4.6 Trasferimenti di dati verso un paese terzo

Il trattamento non è soggetto ad alcun trasferimento di dati verso un paese terzo

4.4.7 Termini previsti per la cancellazione delle diverse categorie di dati

I dati forniti verranno conservati per il tempo necessario al conseguimento delle finalità per le quali sono stati raccolti o per un periodo ulteriore se così disposto dalle norme di diritto, nonché dalle normative in materia di tenuta della documentazione amministrativa o qualora si renda necessario proseguire nell'archiviazione ai fini del pubblico interesse

4.4.8 Ubicazione degli archivi

I dati in formato digitale sono memorizzati all'interno delle postazioni di lavoro assegnate agli uffici e nel server dell'Ente. I dati in formato cartaceo sono custoditi in armadi dotati di serratura

4.5 Sussidi straordinari una tantum

(Fondazione Enpam)

4.5.1 Titolare del trattamento

Denominazione: Fondazione Enpam

Rappresentante: Presidente

DPO: Dott. Giorgio Boni - Piazza Vittorio Emanuele II, n.78 – 00185 Roma - PEC dpo@pec.enpam.it

4.5.2 Descrizione

Gestione amministrativa dei sussidi straordinari erogati dalla Fondazione Enpam a favore degli iscritti dell'Ordine.
In tale ambito, l'ordine redige il parere di ammissibilità e invia la documentazione inerente la richiesta alla Fondazione Enpam

4.5.3 Uffici che trattano i dati

Nessun ufficio specificato

4.5.4 Responsabili del trattamento

Società affidataria del servizio di conservazione digitale sostitutiva
Società affidatarie del servizio di manutenzione dei software di ufficio

Società affidatarie del servizio di manutenzione dell'hardware

4.5.5 Soggetti destinatari

Fondazione Enpam

4.5.6 Trasferimenti di dati verso un paese terzo

Il trattamento non è soggetto ad alcun trasferimento di dati verso un paese terzo

4.5.7 Termini previsti per la cancellazione delle diverse categorie di dati

I dati forniti verranno conservati per il tempo necessario al conseguimento delle finalità per le quali sono stati raccolti o per un periodo ulteriore se così disposto dalle norme di diritto, nonché dalle normative in materia di tenuta della documentazione amministrativa o qualora si renda necessario proseguire nell'archiviazione ai fini del pubblico interesse

4.5.8 Ubicazione degli archivi

I dati in formato digitale sono memorizzati all'interno delle postazioni di lavoro assegnate agli uffici e nel server dell'Ente. I dati in formato cartaceo sono custoditi in armadi dotati di serratura

4.6 Sussidio aggiuntivo

(Fondazione Enpam)

4.6.1 Titolare del trattamento

Denominazione: Fondazione Enpam

Rappresentante: Presidente

DPO: Dott. Giorgio Boni - Piazza Vittorio Emanuele II, n.78 – 00185 Roma - PEC dpo@pec.enpam.it

4.6.2 Descrizione

Gestione amministrativa per l'accesso al sussidio aggiuntivo erogato dalla Fondazione Enpam a favore degli iscritti dell'Ordine. In tale ambito, l'ordine raccoglie la documentazione inerente la richiesta e la trasmette alla Fondazione Enpam

4.6.3 Uffici che trattano i dati

Nessun ufficio specificato

4.6.4 Responsabili del trattamento

Società affidataria del servizio di conservazione digitale sostitutiva
Società affidatarie del servizio di manutenzione dei software di ufficio
Società affidatarie del servizio di manutenzione dell'hardware

4.6.5 Soggetti destinatari

Fondazione Enpam

4.6.6 Trasferimenti di dati verso un paese terzo

Il trattamento non è soggetto ad alcun trasferimento di dati verso un paese terzo

4.6.7 Termini previsti per la cancellazione delle diverse categorie di dati

I dati forniti verranno conservati per il tempo necessario al conseguimento delle finalità per le quali sono stati raccolti o per un periodo ulteriore se così disposto dalle norme di diritto, nonché dalle normative in materia di tenuta della documentazione amministrativa o qualora si renda necessario proseguire nell'archiviazione ai fini del pubblico interesse

4.6.8 Ubicazione degli archivi

I dati in formato digitale sono memorizzati all'interno delle postazioni di lavoro assegnate agli uffici e nel server dell'Ente. I dati in formato cartaceo sono custoditi in armadi dotati di serratura

4.7 Sussidio per calamita' naturali

(Fondazione Enpam)

4.7.1 Titolare del trattamento

Denominazione: Fondazione Enpam

Rappresentante: Presidente

DPO: Dott. Giorgio Boni - Piazza Vittorio Emanuele II, n.78 – 00185 Roma - PEC dpo@pec.enpam.it

4.7.2 Descrizione

Gestione amministrativa per l'accesso al sussidio per calamita' naturali erogato dalla Fondazione Enpam a favore degli iscritti dell'Ordine. In tale ambito, l'ordine raccoglie la documentazione inerente la richiesta e la trasmette alla Fondazione Enpam

4.7.3 Uffici che trattano i dati

Nessun ufficio specificato

4.7.4 Responsabili del trattamento

Società affidataria del servizio di conservazione digitale sostitutiva
Società affidatarie del servizio di manutenzione dei software di ufficio
Società affidatarie del servizio di manutenzione dell'hardware

4.7.5 Soggetti destinatari

Fondazione Enpam

4.7.6 Trasferimenti di dati verso un paese terzo

Il trattamento non è soggetto ad alcun trasferimento di dati verso un paese terzo

4.7.7 Termini previsti per la cancellazione delle diverse categorie di dati

I dati forniti verranno conservati per il tempo necessario al conseguimento delle finalità per le quali sono stati raccolti o per un periodo ulteriore se così disposto dalle norme di diritto, nonché dalle normative in materia di tenuta della documentazione amministrativa o qualora si renda necessario proseguire nell'archiviazione ai fini

del pubblico interesse

4.7.8 Ubicazione degli archivi

I dati in formato digitale sono memorizzati all'interno delle postazioni di lavoro assegnate agli uffici e nel server dell'Ente. I dati in formato cartaceo sono custoditi in armadi dotati di serratura

4.8 Sussidio sostitutivo del reddito

(Fondazione Enpam)

4.8.1 Titolare del trattamento

Denominazione: Fondazione Enpam

Rappresentante: Presidente

DPO: Dott. Giorgio Boni - Piazza Vittorio Emanuele II, n.78 – 00185 Roma - PEC dpo@pec.enpam.it

4.8.2 Descrizione

Gestione amministrativa per l'accesso al sussidio sostitutivo del reddito erogato dalla Fondazione Enpam a favore degli iscritti dell'Ordine. In tale ambito, l'ordine raccoglie la documentazione inerente la richiesta e la trasmette alla Fondazione Enpam

4.8.3 Uffici che trattano i dati

Nessun ufficio specificato

4.8.4 Responsabili del trattamento

Società affidataria del servizio di conservazione digitale sostitutiva
Società affidatarie del servizio di manutenzione dei software di ufficio
Società affidatarie del servizio di manutenzione dell'hardware

4.8.5 Soggetti destinatari

Fondazione Enpam

4.8.6 Trasferimenti di dati verso un paese terzo

Il trattamento non è soggetto ad alcun trasferimento di dati verso un paese terzo

4.8.7 Termini previsti per la cancellazione delle diverse categorie di dati

I dati forniti verranno conservati per il tempo necessario al conseguimento delle finalità per le quali sono stati raccolti o per un periodo ulteriore se così disposto dalle norme di diritto, nonché dalle normative in materia di tenuta della documentazione amministrativa o qualora si renda necessario proseguire nell'archiviazione ai fini del pubblico interesse

4.8.8 Ubicazione degli archivi

I dati in formato digitale sono memorizzati all'interno delle postazioni di lavoro assegnate agli uffici e nel server dell'Ente. I dati in formato cartaceo sono custoditi in armadi dotati di serratura

Art. 54-*bis* del Decreto legislativo 30 marzo 2001, n. 165

Art. 54-*bis* (*Tutela del dipendente pubblico che segnala illeciti)*

1. Il pubblico dipendente che, nell'interesse dell'integrità della pubblica amministrazione, segnala al responsabile della prevenzione della corruzione e della trasparenza di cui all'articolo 1, comma 7, della legge 6 novembre 2012, n. 190, ovvero all'Autorità nazionale anticorruzione (ANAC), o denuncia all'autorità giudiziaria ordinaria o a quella contabile, condotte illecite di cui è venuto a conoscenza in ragione del proprio rapporto di lavoro non può essere sanzionato, demansionato, licenziato, trasferito, o sottoposto ad altra misura organizzativa avente effetti negativi, diretti o indiretti, sulle condizioni di lavoro determinata dalla segnalazione. L'adozione di misure ritenute ritorsive, di cui al primo periodo, nei confronti del segnalante è comunicata in ogni caso all'ANAC dall'interessato o dalle organizzazioni sindacali maggiormente rappresentative nell'amministrazione nella quale le stesse sono state poste in essere. L'ANAC informa il Dipartimento della funzione pubblica della Presidenza del Consiglio dei ministri o gli altri organismi di garanzia o di disciplina per le attività e gli eventuali provvedimenti di competenza.

2. Ai fini del presente articolo, per dipendente pubblico si intende il dipendente delle amministrazioni pubbliche di cui all'articolo 1, comma 2, ivi compreso il dipendente di cui all'articolo 3, il dipendente di un ente pubblico economico ovvero il dipendente di un ente di diritto privato sottoposto a controllo pubblico ai sensi dell'articolo 2359 del codice civile. La disciplina di cui al presente articolo si applica anche ai lavoratori e ai collaboratori delle imprese fornitrici di beni o servizi e che realizzano opere in favore dell'amministrazione pubblica.

3. L'identità del segnalante non può essere rivelata. Nell'ambito del procedimento penale, l'identità del segnalante è coperta dal segreto nei modi e nei limiti previsti dall'articolo 329 del codice di procedura penale. Nell'ambito del procedimento dinanzi alla Corte dei conti, l'identità del segnalante non può essere rivelata fino alla chiusura della fase istruttoria. Nell'ambito del procedimento disciplinare l'identità del segnalante non può essere rivelata, ove la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione, anche se conseguenti alla stessa. Qualora la contestazione sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità del segnalante sia indispensabile per la difesa dell'incolpato, la segnalazione sarà utilizzabile ai fini del procedimento disciplinare solo in presenza di consenso del segnalante alla rivelazione della sua identità.

4. La segnalazione è sottratta all'accesso previsto dagli articoli 22 e seguenti della legge 7 agosto 1990, n. 241, e successive modificazioni.

5. L'ANAC, sentito il Garante per la protezione dei dati personali, adotta apposite linee guida relative alle procedure per la presentazione e la gestione delle segnalazioni. Le linee guida prevedono l'utilizzo di modalità anche informatiche e promuovono il ricorso a strumenti di crittografia per garantire la riservatezza dell'identità del segnalante e per il contenuto delle segnalazioni e della relativa documentazione.

6. Qualora venga accertata, nell'ambito dell'istruttoria condotta dall'ANAC, l'adozione di misure discriminatorie da parte di una delle amministrazioni pubbliche o di uno degli enti di cui al comma 2, fermi restando gli altri profili di responsabilità, l'ANAC applica al responsabile che ha adottato tale misura una sanzione amministrativa pecuniaria da 5.000 a 30.000 euro. Qualora venga accertata l'assenza di procedure per l'inoltro e la gestione delle segnalazioni ovvero l'adozione di procedure non conformi a quelle di cui al comma 5, l'ANAC applica al responsabile la sanzione amministrativa pecuniaria da 10.000 a 50.000 euro. Qualora venga accertato il mancato svolgimento da parte del

responsabile di attività di verifica e analisi delle segnalazioni ricevute, si applica al responsabile la sanzione amministrativa pecuniaria da 10.000 a 50.000 euro. L'ANAC determina l'entità della sanzione tenuto conto delle dimensioni dell'amministrazione o dell'ente cui si riferisce la segnalazione.

7. È a carico dell'amministrazione pubblica o dell'ente di cui al comma 2 dimostrare che le misure discriminatorie o ritorsive, adottate nei confronti del segnalante, sono motivate da ragioni estranee alla segnalazione stessa. Gli atti discriminatori o ritorsivi adottati dall'amministrazione o dall'ente sono nulli.

8. Il segnalante che sia licenziato a motivo della segnalazione è reintegrato nel posto di lavoro ai sensi dell'articolo 2 del decreto legislativo 4 marzo 2015, n. 23.

9. Le tutele di cui al presente articolo non sono garantite nei casi in cui sia accertata, anche con sentenza di primo grado, la responsabilità penale del segnalante per i reati di calunnia o diffamazione o comunque per reati commessi con la denuncia di cui al comma 1 ovvero la sua responsabilità civile, per lo stesso titolo, nei casi di dolo o colpa grave.

****

Art. 3 della Legge 30 novembre 2017, n. 179

Art. 3 *(Integrazione della disciplina dell'obbligo di segreto d'ufficio, aziendale, professionale, scientifico e industriale)*

1. Nelle ipotesi di segnalazione o denuncia effettuate nelle forme e nei limiti di cui all'articolo 54-*bis* del decreto legislativo 30 marzo 2001, n. 165, e all'articolo 6 del decreto legislativo 8 giugno 2001, n. 231, come modificati dalla presente legge, il perseguimento dell'interesse all'integrità delle amministrazioni, pubbliche e private, nonché alla prevenzione e alla repressione delle malversazioni, costituisce giusta causa di rivelazione di notizie coperte dall'obbligo di segreto di cui agli articoli 326, 622 e 623 del codice penale e all'articolo 2105 del codice civile.

2. La disposizione di cui al comma 1 non si applica nel caso in cui l'obbligo di segreto professionale gravi su chi sia venuto a conoscenza della notizia in ragione di un rapporto di consulenza professionale o di assistenza con l'ente, l'impresa o la persona fisica interessata.

3. Quando notizie e documenti che sono comunicati all'organo deputato a riceverli siano oggetto di segreto aziendale, professionale o d'ufficio, costituisce violazione del relativo obbligo di segreto la rivelazione con modalità eccedenti rispetto alle finalità dell'eliminazione dell'illecito e, in particolare, la rivelazione al di fuori del canale di comunicazione specificamente predisposto a tal fine.

OMCeOCampobasso
Ordine Provinciale dei Medici-Chirurghi e degli Odontoiatri

ORDINE PROVINCIALE DEI MEDICI-CHIRUGHI E DEGLI ODONTOIATRI DELLA PROVINCIADI CAMPOBASSO

Via Mazzini, 129/A - Campobasso (CB)
PEC:info.cb@pec.omceo.it TELEFONO: 0874.69177

GDPR

DATA BREACH

GESTIONE DELLE VIOLAZIONI

Procedura di notifica delle violazioni e registro dei data breach

Informazione di Revisione

Revisione	*Data*	*Note*
A		Prima stesura

1. L'evento di violazione dei dati e l'obbligatorietà della notifica

Il Data Breach rappresenta un evento di violazione dei dati che può avere sia origine **dolosa** (*come ad es. un attacco informativo*) che **accidentale** (*come un accesso abusivo, un incidente, ecc.*).

Per essere catalogato come Data Breach l'evento di violazione deve ad ogni nodo comportare la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o trattati".

La violazione è classificabile in:

- "**violazione della riservatezza**", in caso di accesso o divulgazione di dati personali non autorizzata o accidentale;
- "**violazione dell'integrità**", in caso di modifica non autorizzata o accidentale di dati personali;
- "**violazione della disponibilità**", in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali.

Ai sensi dell'Art. 33 del GDPR, un evento di violazione dei dati personali, ovvero Data Breach, deve essere notificato, entro le 72 ore dal momento in cui se ne è venuto a conoscenza, all'autorità di controllo (leggi Garante della Privacy), a meno che sia improbabile che esso comporti un rischio per i diritti e le libertà delle persone fisiche.

L'Art. 34 dispone, altresì, che quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, l'accadimento deve essere comunicato, senza ingiustificato ritardo, anche all'interessato, ossia la persona fisica che è identificata dai dati oggetto di violazione.

2. Procedure e misure specifiche

Seguono le procedure interne, rappresentate nelle diverse fasi, da adottare necessariamente in caso di evento di violazione dei dati personali.

FASE 1 – Segnalazione e raccolta delle informazioni

Descrizione
Il Titolare del Trattamento o il DPO riceve una segnalazione di avvenuta violazione di dati personali, che può pervenire dal personale dell'Ente, da soggetti esterni, anche non interessati, o da un Responsabile del Trattamento.

Azioni da intraprendere
Il Titolare del Trattamento, eventualmente con l'ausilio del DPO, prende in carico la segnalazione e coinvolgendo le figure tecniche interessate, designati e eventualmente responsabili del trattamento, attiva la procedura di analisi e valutazione dell'evento.

FASE 2 – Compilazione della scheda evento e istituzione del tavolo tecnico di valutazione

Descrizione
Il Titolare del Trattamento, a seguito della segnalazione di avvenuta violazione dei dati personali compila la scheda evento e istituisce il tavolo tecnico di valutazione.

Azioni da intraprendere

1. Il Titolare del Trattamento compila la Scheda Evento (Allegato N. 1) e la inoltra al DPO attraverso posta elettronica certificata. La scheda evento verrà compilata nelle seguenti parti: data e ora di compilazione della scheda, segnalante, luogo della violazione, data e ora dell'evento (anche solo presunta), data e ora in cui si è avuta conoscenza della violazione, fonte della segnalazione e descrizione dell'evento.
2. Il Titolare del Trattamento istituisce il tavolo tecnico per la valutazione della segnalazione, al quale dovranno partecipare:
    - il DPO;
    - i soggetti designati al trattamento dei dati personali oggetto della presunta violazione;
    - l'eventuale responsabile del trattamento se coinvolto.

FASE 3 – Verifica preliminare

Descrizione
Il tavolo tecnico costituito dal Titolare del Trattamento inizia il processo di verifica della segnalazione di violazione di dati personali.

Azioni da intraprendere
Il tavolo tecnico procede a una prima analisi della segnalazione al fine di verificare se essa rappresenti un "falso positivo".
Nel caso in cui l'evento segnalato risulti essere un falso positivo, l'incidente viene chiuso e riportato come tale dal Titolare del Trattamento nel Registro dei Data Breach (Allegato N. 3), nella apposita sezione dedicata agli "eventi falsi positivi".
Nel caso in cui venga invece accertata una effettiva violazione dei dati personali i partecipanti al tavolo tecnico recuperano le informazioni di dettaglio necessarie per completare la Scheda Evento nelle parti non compilate nella Fase 2.

FASE 4 – Valutazione dei rischi

Descrizione
L'evento di violazione non rappresenta un falso positivo. Si procede alla valutazione dei rischi.

Azioni da intraprendere
Il tavolo tecnico procede alla valutazione dell'evento accertato al fine di determinarne gli elementi

caratterizzanti e, di conseguenza, il rischio per le libertà e i diritti degli Interessati.

Sarà quindi compilata la Scheda Violazione Dati (Allegato N.2) e valutato il livello di rischio (NULLO, BASSO, MEDIO, ALTO) riferito alla probabilità che si verifichi una delle seguenti condizioni a danno di persone fisiche, anche diverse dall'Interessato, alle quali si riferiscono i dati:

- discriminazioni;
- furto o usurpazione d'identità;
- pregiudizio alla reputazione;
- perdita di riservatezza dei dati personali protetti da segreto professionale;
- decifratura non autorizzata della pseudonimizzazione;
- danno economico o sociale significativo;
- privazione o limitazione di diritti o libertà;
- danni fisici, materiali o immateriali, alle persone fisiche.

Concorreranno alla valutazione del livello di rischio il verificarsi delle seguenti circostanze:

- la violazione ha interessato dati idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché di dati genetici, dati relativi alla salute o dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza;
- la violazione ha interessato dati capaci di consentire la valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali;
- la violazione ha interessato dati riguardanti persone fisiche vulnerabili, in particolare minori;
- la violazione ha interessato una notevole quantità di Dati Personali;
- la violazione ha interessato un vasto numero di Interessati.

Qualora il livello di rischio non venga valutato come NULLO il tavolo tecnico provvede, tempestivamente, ad adottare le opportune misure volte a minimizzare le conseguenze negative della violazione.

FASE 5 – Notifica al garante

Descrizione
Il livello di rischio non è valutato come NULLO. Il Titolare dei trattamenti notifica la violazione all'Autorità di Controllo.

Azioni da intraprendere
Il Titolare del Trattamento, entro le **72 ore** dal momento in cui è venuto a conoscenza della violazione, comunica l'evento all'Autorità di Controllo competente.

La comunicazione avverrà mediante il servizio telematico raggiungibile alla URL https://servizi.gpdp.it/databreach/s/

Eccezioni

1. Il Titolare del Trattamento procede a una notifica per fasi qualora egli non disponga di tutte le informazioni necessarie a descrivere esaustivamente l'accaduto.
2. Qualora il Titolare del Trattamento non riesca a notificare l'evento entro le 72 ore stabilite, egli espone, all'interno della stessa comunicazione, le cause dell'impedimento.

FASE 6 – Comunicazione della violazione all'Interessato

Descrizione

Il livello di rischio è valutato come ALTO. Il Titolare del Trattamento comunica l'accaduto anche agli Interessati poiché la violazione comporta un elevato pericolo per i diritti e le libertà.

Azioni da intraprendere

Il Titolare del Trattamento comunica a tutti gli interessati, senza ingiustificato ritardo, dell'avvenuto evento di violazione dei dati personali.

La comunicazione è inoltrata attraverso i canali ritenuti maggiormente idonei. Qualora essa richieda sforzi sproporzionati, procede a una comunicazione pubblica o a una misura simile che garantisca analoga efficacia.

La comunicazione contiene le seguenti informazioni:

- data e ora della violazione, anche solo presunta, e data e ora in cui si è avuto conoscenza della stessa;
- natura della violazione dei dati personali;
- nome e dati di contatto del DPO o di altro punto di contatto presso cui ottenere più informazioni;
- le probabili conseguenze della violazione dei dati personali;
- una descrizione sintetica delle misure adottate o di cui si propone l'adozione per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi.

Eccezioni

Il Titolare del Trattamento non comunica l'accadimento agli interessati se, successivamente, procede all'adozione di misure atte a scongiurare il sopraggiungere del rischio elevato per i diritti e le libertà delle persone fisiche. Dette misure sono documentate nella scheda di violazione.

FASE 7 – Annotazione nel registro del data breach

Descrizione

Il Titolare del Trattamento documenta all'interno del Registro di Data Breach l'evento di violazione dei dati personali.

Azioni da intraprendere

Il Titolare del Trattamento annota all'interno del Registro di Data Breach l'evento di violazione dei dati personali.

ALLEGATO N. 1 – SCHEDA EVENTO

SCHEDA EVENTO N. _____			
DATI GENERALI			
Data di compilazione		**Ora di compilazione**	
Fonte della segnalazione	Rilevazione da parte del titolare ☐ Comunicazione del responsabile del trattam. ☐ Segnalazione da parte di un interessato ☐ Segnalazione da parte di un soggetto esterno ☐ Notizie stampa ☐ Altro ☐	**Soggetto ricevente la segnalazione**	Titolare del Trattamento ☐ DPO ☐
Soggetto segnalante			
Data e ora in cui si è avuta conoscenza della violazione			
DESCRIZIONE DELL'EVENTO			
Sede della violazione			
Data e ora della violazione		**La data dell'evento è presunta**	SI☐ NO ☐
Descrizione dell'evento			
Numerosità dei dati personali di cui si presume la violazione [(1)]		**Numero di interessati coinvolti**	
Descrizione dei sistemi di elaborazione e/o memorizzazione dei dati coinvolti [(2)]			

Istruzioni di compilazione

[(1)] *Inserire un valore numerico quale, ad esempio, il numero di fatture, ordini, referti, immagini, record di un database o il numero di transazioni.*

[(2)] *Specificare il dispositivo tecnologico interessato dalla violazione quale, ad esempio, unità server, personal computer, notebook, chiavetta USB, smarphone. Inidcare, altresì, la loro ubicazione riferita al momento della violazione.*

ALLEGATO N. 2 – SCHEDA VIOLAZIONE DATI

IDENTIFICATIVO DELL'EVENTO – SCHEDA EVENTO N. _____ (1)	
DATI GENERALI	
Nominativi e firme dei componenti del tavolo tecnico	
DESCRIZIONE DELL'EVENTO	
Natura della violazione	Perdita di riservatezza ☐ Perdita di integrità ☐ Perdita di disponibilità ☐
Data e ora della violazione	Azione intenzionale interna ☐ Azione accidentale interna ☐ Azione intenzionale esterna ☐ Azione accidentale esterna ☐
Misure tecniche e organizzative in essere al momento della violazione	
Categorie di interessati coinvolti nella violazione (2)	
Categorie di dati personali coinvolti	Dati Anagrafici ☐ Dati di contatto ☐ Dati di accesso e di identificazione ☐ Dati di pagamento ☐ Dati inerenti servizi di comunicazione ☐ Dati giudiziari ☐ Dati di profilazione ☐ Dati in documenti di identificaz. ☐ Dati di origine razziale o etnica ☐ Opinioni politiche ☐ Convinzioni religiose o filosofiche ☐ Appartenenza sindacale ☐ Dati atti a rivelare la vita sessuale ☐ Orientamento sessuale ☐ Dati relativi alla salute ☐ Dati genetici ☐ Dati Biometrici ☐ Dati di ubicazione ☐
Descrizione di dettaglio delle categorie di dati personali oggetto della violazione per ciascuna categoria di interessati	
VALUTAZIONE DELLE CONSEGUENZE	
Perdita di riservatezza	I dati sono stati divulgati al di fuori di quanto previsto dall'informativa ☐ I dati possono essere correlati, senza sforzo irragionevole, ad altre informazioni relative agli interessati ☐

	I dati possono essere utilizzati per finalità diverse da quelle previste oppure in modo non lecito ☐
Perdita di integrità	I dati sono stati modificati e resi inconsistenti ☐ I dati sono stati modificati mantenendo la consistenza ☐
Perdita di disponibilità	Mancato accesso a servizi ☐ Malfunzionamento e difficoltà nell'utilizzo di servizi ☐
Ulteriori indicazioni sulle conseguenze	

VALUTAZIONE DELL'IMPATTO

Tipologia di impatto	Perdita del controllo dei dati ☐ Limitazione dei diritti ☐ Discriminazione ☐ Furto o usurpazione d'identità ☐ Frodi ☐ Perdite finanziarie ☐ Decifratura non autorizzata ☐ Pregiudizio alla reputazione ☐ Perdita di riservatezza di dati protetti da segreto professionale ☐ Conoscenza da parte di terzi non autorizzati ☐ Danno economico o sociale significativo di qualsiasi natura ☐
Gravità	Trascurabile ☐ Bassa ☐ Media ☐ Alta ☐
Motivazioni della valutazione della gravità	

MISURE ADOTTATE A SEGUITO DELLA VIOLAZIONE

Misure tecniche e organizzative adottate, o di cui si propone l'adozione, per porre rimedio alla violazione e attenuarne i possibili effetti negativi per gli interessati	
Misure tecniche e organizzative adottate, o di cui si propone l'adozione, per prevenire simili violazioni future	

VALUTAZIONE DEL RISCHIO PER GLI INTERESSATI

Indicazione di valutazione	La violazione è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche ☐

	La violazione non è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche ☐	
Motivazioni della valutazione del rischio		
COMUNICAZIONE DELLA VIOLAZIONE AGLI INTERESSATI		
Si procede alla comunicazione ☐	Non si procede alla comunicazione ☐	
Indicazioni sull'eventuale comunicazione agli interessati	Numero di interessati	
	Canale utilizzato	SMS ☐ Posta cartacea ☐ Posta elettronica ☐ Comunicazione pubblica ☐ Altro ☐
	Descrizione delle modalità di comunicazione	
Motivazioni sulla decisione di non procedere alla comunicazione agli interessati	☐ La violazione non è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche ☐ Sono state adottate, successivamente, misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati	
	Descrizione delle misure attuate	

Istruzioni di compilazione

(1) Riportare il numero della scheda evento compilata nelle precedenti fasi.

(2) Esprimere gli interessati coinvolti in termini di categoria quali ad esempio: Dipendenti/Consulenti, Clienti, Associati, soci, Soggetti che ricoprono cariche sociali, Beneficiari o assistiti, Minori, Persone vulnerabili (es. vittime di violenze o abusi, rifugiati, richiedenti asilo).

(3) Da compilare solo se sono state adottate misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati.

OMCeOCampobasso
Ordine Provinciale dei Medici-Chirurghi e degli Odontoiatri

ALLEGATO N. 3 – REGISTRO DEGLI EVENTI DI DATA BREACH

Istruzioni di compilazione

(1) Riportare il numero della Scheda Evento prodotta nella Fase 2.
(2) P=Falso Positivo, IRR=Irrilevante, RIL=Rilevante
(3) RISER=Perdita di riservatezza, INTEG=Perdita di integrità, DISP=Perdita di disponibilità.
(4) Specificare la modalità utilizzata per la comunicazione quali ad esempio SMS, Posta cartacea, Posta elettronica, Comunicazione pubblica

REGISTRO DEGLI EVENTI DI VIOLAZIONE DEI DATI PERSONALI

Aggiornato alla data del _____

Riferimenti dell'evento				Conseguenze (3)	Azioni adottate			
Numero scheda evento (1)	Data	Valutazione (2)	Descrizione sintetica		Notifica autorità di controllo (SI/NO)	Comunicazione Interessato		
						SI/NO	Data	Modalità