MANUALE DI GESTIONE DOCUMENTALE

Firmato da: (Q con FEQ) (A con FEA)
1 - Damia Valentina A (30/06/2025) 2 - Bacocco Duilio Luca Q (30/06/
3 - Villanacci Carlo A (30/06/2025) 4 - Stefano Anna A (30/06/2025)

Per la verifica di conformità del Contrassegno Elettronico apposto è possibile scaricare il documento, conforme al DPCM 13/11/2014, tramite l'App Honos.
Visita https://honos.land.it/ per le istruzioni.

Sommario

CAPITOLO I 5
1. PRINCIPI GENERALI 5
1.1. Premesse 5
1.2. Ambito di applicazione 5
1.3. Riferimenti normativi 6
1.4. Tutela dei dati personali: GDPR e D. Lgs. 196/2003 e ss.mm.ii. e prassi comportamentale dell'Utente di protocollo 8
1.5. Area Organizzativa Omogenea e modello organizzativo 9
1.6. Ufficio per la gestione del protocollo informatico 9
1.7. Definizioni 10
1.8. Il Responsabile della Gestione Documentale (RGD) 10
1.9. Profili di abilitazione alle informazioni del sistema di gestione documentale 11
1.10. Accreditamento all'IPA e casella di posta elettronica certificata dell'Ufficio Protocollo 11
1.11. Altre caselle di posta elettronica istituzionale certificata e non certificata 12
1.12. Prescrizioni conseguenti all'avvio del sistema di protocollo informatico e cessazione dei cosiddetti "protocolli interni" 12
1.13 Gestione della sicurezza informatica 12
CAPITOLO II 13
2. ELEMENTI CARATTERIZZANTI IL PROTOCOLLO INFORMATICO 13
2.1. Natura giuridica del Protocollo informatico 13
2.2. Unicità del protocollo informatico 13
2.3. Unicità, immodificabilità e conservazione del protocollo informatico 13
2.4. Contenuti minimi del Registro giornaliero di protocollo 14
CAPITOLO III 15
3. IL DOCUMENTO 15
3.1. Documento amministrativo 15
3.2. Documento informatico 15
3.3. Documento analogico 15
3.4. Documenti prodotti dall'ISS 15
3.5. Documenti in ingresso 16
3.6. Documenti in uscita 16

3.7. Documenti interni 16
3.8. Duplicato, copia ed estratto di documenti informatici 16
3.9. Metadati 17
CAPITOLO IV 18
4. GESTIONE DELLA CORRISPONDENZA IN ENTRATA 18
4.1. Regole generali di assegnazione e smistamento dei documenti 18
4.2. Ricezione di documenti analogici 18
4.3. Ricezione di documenti informatici 18
4.4. Errata ricezione di documenti analogici 19
4.5. Errata ricezione di documenti informatici 19
4.6. Rilascio di ricevute attestanti la ricezione di documenti analogici 19
4.7. Rilascio di ricevute attestanti la ricezione di documenti informatici 20
4.8. Termini per la registrazione di protocollo 20
4.9. Differimento dei termini di registrazione 20
4.10. Registrazione e segnatura dei documenti in entrata 20
4.11. Diritto di accesso e tutela dei dati personali 21
CAPITOLO V 22
5. GESTIONE DELLA CORRISPONDENZA IN USCITA 22
5.1. Regole generali 22
CAPITOLO VI 23
6. GESTIONE DI CATEGORIE PARTICOLARE DI CORRISPONDENZA 23
6.1. Corrispondenza riservata 23
6.2. Documenti indirizzati nominalmente al personale dell'Istituto 23
6.3. Documenti anonimi o privi di sottoscrizione 24
6.4. Documenti con più destinatari 24
6.5. Protocollazione di un numero consistente di documenti 24
6.6. Protocolli urgenti 24
6.7. Integrazioni documentarie 24
CAPITOLO VII 25
7. FASCICOLAZIONE DEI DOCUMENTI 25
7.1. Fascicolazione dei documenti 25
CAPITOLO VIII 26

8. REGISTRO DI EMERGENZA E CHIUSURA REGISTRO DI PROTOCOLLO 26
8.1. Registro di emergenza 26
CAPITOLO IX 27
9. ORGANIZZAZIONE E GESTIONE DELL'ARCHIVIO 27
9.1. Archivio e sue partizioni cronologiche 27
9.2. Trasferimento dei documenti dall'archivio corrente a quello di deposito 27
9.3. L'archivio storico 27

CAPITOLO I

1. PRINCIPI GENERALI

1.1. Premesse

Il presente Manuale di Gestione Documentale (di seguito MGD) è redatto in conformità a quanto indicato dalle *Linee Guida sulla formazione, gestione e conservazione dei documenti informatici* del maggio 2021 redatte dall'Agenzia per l'Italia Digitale (AgID) (d'ora in avanti Linee Guida), che contengono le regole tecniche sugli ambiti disciplinati dalle disposizioni del Codice dell'Amministrazione Digitale ex decreto legislativo 7 marzo 2005 n. 82 e s.m.i. (d'ora in avanti CAD), e più precisamente dagli artt. da 20 a 23-quater, 34, da 40 a 47, da 49 a 51, 64-bis, 65, e costituiscono la nuova versione aggiornata delle regole tecniche in materia di formazione, protocollazione, gestione e conservazione del documento, già precedentemente regolate dal DPCM 13 novembre 2014 contenente "Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici" e dal DPCM 3 dicembre 2013 contenente "Regole tecniche in materia di sistema di conservazione", entrambi abrogati dalla data di applicazione delle Linee Guida.
Le Linee Guida hanno abrogato tutte le disposizioni del DPCM 3 dicembre 2013 contenente "Regole tecniche per il protocollo informatico", fatta eccezione per gli artt. 2 comma 1, 6, 9, 18 commi 1 e 5, 20 e 21.
Sempre a far data dall'applicazione delle Linee Guida è stata abrogata la circolare n. 60 del 23 gennaio 2013 di AgID in materia di "Formato e definizione dei tipi di informazioni minime ed accessorie associate ai messaggi scambiati tra le Pubbliche Amministrazioni", che è stata sostituita dall'allegato 6 "Comunicazioni tra AOO di documenti amministrativi protocollati" delle Linee Guida.
Secondo quanto previsto nel paragrafo 3.5 delle Linee Guida, il MGD descrive il sistema di gestione informatica dei documenti e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.
Si tratta, in sostanza, di uno strumento operativo che descrive il ciclo di vita dei documenti, analogici e digitali.
Il suo obiettivo è descrivere le funzionalità disponibili per gli addetti al servizio e per eventuali soggetti esterni che, a diverso titolo, interagiscono con le Aree Organizzative Omogenee (AOO) dell'Istituto Superiore di Sanità (di seguito ISS), dalla fase di protocollazione (in entrata, in uscita e interna) alla fase di archiviazione.
Il MGD disciplina, pertanto, le attività di formazione, registrazione, classificazione e fascicolazione dei documenti di varia natura prodotti dall'ISS, nell'espletamento delle proprie funzioni istituzionali.
Ciò premesso, il presente MGD è destinato alla più ampia diffusione e conoscenza, sia interna che esterna.

1.2. Ambito di applicazione

Il MGD descrive le attività di formazione, protocollazione, gestione e conservazione dei documenti, nonché la gestione dei flussi documentali ed archivistici in relazione ai procedimenti di competenza dell'ISS.
In particolare, vengono disciplinate le seguenti procedure:

- classificazione dei documenti in entrata e in uscita dall'ISS sulla base di un Piano di classificazione, c.d. Titolario che indica in che modo i diversi documenti prodotti in entrata

e in uscita debbano essere classificati e ordinati all'interno di un dato archivio, per assicurare una stratificazione ordinata;

- gestione, da parte dell'Ufficio preposto al protocollo informatico, della documentazione in entrata, con successiva assegnazione della stessa, agli Uffici amministrativi e alle diverse Strutture scientifiche competenti alla trattazione dell'argomento;
- gestione della documentazione in uscita dalle Unità organizzative dell'ISS;
- formazione dei fascicoli, prodromica ad una corretta gestione archivistica.

Il MGD è corredato da due allegati:

1. All. 1 - Il **Massimario di selezione, conservazione e scarto**
2. All. 2 - Il **Piano di Classificazione o Titolario**

1.3. Riferimenti normativi

Atto	**data**	**contenuti**
R.D. n. 1163	1911	Regolamento per gli archivi di Stato
D.P.R. n. 1409	1963	Norme relative all'ordinamento ed al personale degli archivi di Stato
L. n. 241	07/08/1990	Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi.
D.P.R. n. 445	28/12/2000	Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (TUDA)
D.P.R. 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 n. 196	30/06/2003	Codice in materia di protezione dei dati personali
L. n. 4	09/01/2004 aggiornata dal D. Lgs 10 agosto 2018 n. 106	Disposizioni per favorire l'accesso dei soggetti disabili agli strumenti informatici.
D. Lgs. n. 82	07/03/2005	Codice dell'amministrazione digitale, c.d. CAD e successive modificazioni
D.P.R. n. 633/1972 art. 39	in vigore dal 01/01/ 2013	Modificato da: L. n. 228 del 24/12/2012, Art. 1 – Le fatture elettroniche in formato elettronico e quelle cartacee possono essere conservate elettronicamente
D.P.C.M.	22/02/2013	Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali.
D. Lgs. n. 33	14/03/2013	Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni.
D.P.C.M.	21/03/2013	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
D.P.C.M.	03/12/2013	Regole tecniche per il protocollo informatico. **Abrogate dalle Linee Guida AGiD (maggio 2021) tutte le disposizioni fatti salvi**: • Articolo 2, comma1 • Articolo 6 • Articolo 9 • Articolo 18, commi 1 e 5 • Art. 20 • Art. 21
Reg. UE n. 910	23/07/2014	Identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE (eIDAS).
Reg. UE 679/2016 GDPR - General Data Protection	27/04/2016	Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, 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 (GDPR)
Circolare dell'Agenzia per l'Italia Digitale - AgID n. 2	18/04/2017	Misure minime di sicurezza ICT per la PA
Circolare n. 2 dell'AGiD	09/04/2018	Criteri per la qualificazione dei Cloud Service Provider per la PA
Circolare n. 3 dell'AGiD	09/04/2018	Criteri per la qualificazione di servizi SaaS per il Cloud della PA
Regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio	2018	Quadro applicabile alla libera circolazione dei dati non personali dell'Unione europea
D.P.C.M. n. 76	19/06/2019	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	09/01/2020	Accessibilità degli strumenti informatici
AGID – Agenzia per l'Italia digitale	2021	Linee guida sulla formazione, gestione e conservazione dei documenti informatici
AGID – Agenzia per l'Italia digitale	2022	Vademecum per l'implementazione delle Linee guida sulla formazione, gestione e conservazione dei documenti informatici

AGID – Agenzia per l'Italia digitale	2022	Modelli di interoperabilità tra sistemi di conservazione
AGID – Agenzia per l'Italia digitale	2023	La conservazione delle basi dati
AGID – Agenzia per l'Italia digitale	2024	Piano Triennale per l'Informatica nella Pubblica Amministrazione 2024-2026,

1.4. Tutela dei dati personali: GDPR e D. Lgs. 196/2003 e ss.mm.ii. e prassi comportamentale dell'Utente di protocollo

L'ISS è un Ente Pubblico di Ricerca e quando produce documentazione che contiene dati personali deve ottemperare al Regolamento Generale per la Protezione dei Dati Personali (GDPR) all'atto della protocollazione. In particolare, gli addetti autorizzati ad accedere al sistema di protocollo informatico (protocollatori), incaricati dal Responsabile della Gestione Documentale (RGD), devono seguire norme comportamentali definite dall'incarico espletato:

- obbligo di riservatezza per ciò che riguarda tutto il materiale che viene gestito durante le attività di protocollazione, con particolare attenzione rivolta alla prevenzione della divulgazione di dati e di informazioni strettamente personali;
- divieto di condivisione delle credenziali di accesso, da mantenersi strettamente personali e segrete; è altresì proibito consentire l'uso del sistema ad altri per mezzo delle proprie credenziali (es. soggetto terzo che protocolla utilizzando il sistema cui ha già fatto accesso un altro utente);
- qualora fosse necessario sospendere un'operazione di protocollazione, allontanandosi dalla postazione in uso, è obbligatorio lasciare la postazione "bloccata" per evitare che terzi possano accedere indebitamente alle informazioni in fase di inserimento o in generale a dati presenti nel sistema di protocollo.

Inoltre, l'ISS garantisce che i documenti trasmessi sia all'interno che all'esterno dell'Ente riportino le sole informazioni strettamente necessarie per il perseguimento delle finalità istituzionali.
L'ISS, in conformità al GDPR, ha adottato misure tecniche e organizzative adeguate al fine di garantire, ed essere in grado di dimostrare, la conformità dei trattamenti al Regolamento, tenendo conto della natura, dell'ambito di applicazione, del contesto, e delle finalità degli stessi, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche. Dette misure vengono periodicamente riesaminate ed aggiornate (Art. 32 GDPR).
L'assetto organizzativo privacy adottato prevede l'attribuzione di specifiche funzioni e compiti connessi al trattamento dei dati personali, ai sensi degli artt. 29 Regolamento UE 2016/679 (GDPR/RGPD) e 2– quaterdecies del Decreto Legislativo 30/6/2003, n. 196, come modificato dal Decreto Legislativo 10/8/2018, n.101 (cd Nuovo Codice Privacy), ss.mm.ii., al fine di creare un Organigramma privacy dell'Ente a struttura piramidale.
Secondo quanto definito nell'art. 5 del GDPR e considerato il fatto che le Pubbliche Amministrazioni devono avere un sistema documentale in grado di sostenere quanto definito nel Regolamento Europeo stesso e rispettare il principio di tracciabilità dell'azione amministrativa, bisogna:

- identificare in modo univoco ogni documento creato o acquisito mediante la registrazione di informazioni descrittive e la sua classificazione, utili per facilitare il recupero e comprovare l'esistenza del documento (elementi contenuti nel sistema di protocollo informatico);

- definire i diritti di accesso ai documenti in base ai dati ed alle informazioni contenute, attribuendo a ciascun utente di protocollo permessi adeguati e sufficienti allo svolgimento delle attività assegnate;
- stabilire i tempi di conservazione a partire dalla creazione della documentazione, elaborando un piano di conservazione;
- prevedere sistemi di tracciabilità dei dati e dei documenti attraverso una infrastruttura informatica avanzata.

Si ricorda che i sistemi di gestione documentale dovrebbero essere in grado di limitare i rischi che minacciano i dati e le informazioni contenute nei documenti amministrativi.
Le condizioni di cui sopra devono essere applicate anche ai sistemi di conservazione, in modo da garantire rintracciabilità, integrità e riservatezza dei documenti nel rispetto dei principi definiti dal Regolamento Europeo.

1.5. Area Organizzativa Omogenea e modello organizzativo

Ai sensi di quanto disposto dall'art. 50 c. 4 del DPR 445/2000 "Ciascuna amministrazione individua, nell'ambito del proprio ordinamento, gli uffici da considerare ai fini della gestione unica o coordinata dei documenti per grandi aree organizzative omogenee, assicurando criteri uniformi di classificazione e archiviazione, nonché di comunicazione interna tra le aree stesse".
Per la gestione dei flussi documentali, l'ISS ha individuato un'unica Area Organizzativa Omogenea (AOO), ove è istituito un univoco servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e dell'archivio.

1.6. Ufficio per la gestione del protocollo informatico

All'interno dell'Amministrazione, il sistema archivistico è unico ed il sistema di protocollazione è centralizzato, in quanto tutta la corrispondenza viene protocollata e classificata dalla sola *Area archivio e protocollo centrali* dell'ISS, quale Area organizzativa preposta alla gestione del protocollo informatico, dei flussi documentali (analogici e digitali) e dell'archivio, all'interno dell'Ufficio I-Affari Generali, facente capo alla Direzione Centrale degli Affari Generali (DIRAG), ex art. 21 del vigente Regolamento di Organizzazione e Funzionamento (ROF) dell'ISS.
Ciò premesso, ai sensi dell'art. 61, c. 3, del DPR 445/2000, il servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, facente capo alla citata *Area archivio e protocollo centrali* dell'Ufficio I-Affari Generali svolge i seguenti compiti:

a) attribuisce il livello di autorizzazione per l'accesso alle funzioni della procedura, distinguendo tra abilitazioni alla consultazione e abilitazioni all'inserimento e alla modifica delle informazioni, abilitando pertanto il personale dell'Ente all'attività di protocollazione e all'utilizzo dei relativi strumenti informatici, assegnando le autorizzazioni alle operazioni secondo il principio del privilegio minimo assegnato (PoLP, principle of least privilege);
b) garantisce il rispetto delle disposizioni del DPR 445/2000 durante le operazioni di registrazione e di segnatura di protocollo;
c) assicura la corretta produzione e conservazione del registro giornaliero di protocollo di cui all'art. 53 del medesimo DPR 445/2000;
d) cura le funzionalità del sistema informatico di protocollo in collaborazione con i servizi di gestione dei sistemi informativi affinché, in caso di guasti o anomalie del sistema, le ordinarie attività siano ripristinate entro ventiquattro ore dal blocco o, comunque, nel più breve tempo possibile;

e) conserva, attraverso i servizi di gestione dei sistemi informativi, 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;
f) garantisce il buon funzionamento degli strumenti ed il rispetto delle procedure concernenti le attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, incluse le funzionalità di accesso di cui agli artt. 59 e 60 del DPR 445/2000 e le attività di gestione degli archivi di cui ai successivi artt. 67, 68 e 69 del medesimo Decreto;
g) autorizza, con idonei provvedimenti, le eventuali operazioni di annullamento delle registrazioni di protocollo, ai sensi dell'art. 54 del DPR 445/2000, apre e chiude il registro di protocollazione di emergenza;
h) vigilia sull'osservanza delle disposizioni del DPR 445/2000 da parte del personale autorizzato e degli incaricati.

1.7. Definizioni

Al fine di agevolare la comprensione del presente MGD, si riportano di seguito gli acronimi utilizzati:
ISS – Istituto Superiore di Sanità
AOO – Area Organizzativa Omogenea, intesa quale insieme di strutture organizzative che si caratterizzano per una gestione coordinata ed unitaria della documentazione, ai sensi dell'art.50, c. 4 del DPR 445/2000
AAPC – Area Archivio e Protocollo Centrali, quale unità organizzativa, all'interno dell'Ufficio I Affari Generali, della Direzione Centrale Affari Generali (DIRAG), preposta alla gestione del protocollo informatico, dei flussi documentali e dell'archivio
RGD – Responsabile della Gestione Documentale, che nell'ISS, allo stato attuale, coincide con il Dirigente dell'AAPC (di seguito sempre RGD)
UO – Unità organizzativa, ovvero Uffici Amministrativi di livello dirigenziale, nonché Strutture tecnico-scientifiche in cui si articola l'AOO

1.8. Il Responsabile della Gestione Documentale (RGD)

La figura del RGD (o Responsabile del Servizio per la gestione informatica dei documenti, dei flussi documentali e degli archivi) è stata introdotta dall'art. 61 del DPR n. 445/2000, che dispone per le pubbliche amministrazioni l'istituzione, all'interno delle aree organizzative omogenee identificate (AOO), di un apposito servizio per la tenuta del protocollo informatico, dei flussi documentali e degli archivi, da affidare a un dirigente o a un funzionario in possesso di idonei requisiti professionali o di professionalità tecnico-archivistica.
Il RGD, per avere un sistema di gestione documentale aderente alla normativa vigente in materia, deve definire i diritti di accesso ai documenti in base ai dati personali trattati.
Per questo deve fornire delle regole a tutti coloro che vengono in possesso o trattino dati personali, che rispettino il Reg. n. 2016/679/UE e il Codice di Comportamento per i dipendenti delle Pubbliche Amministrazioni di cui ogni Ente dotarsi (art. 54 c.5 del D. lgs n. 165 del 2001).
In particolare, rientra nei compiti del RGD:

1) prevedere adeguati meccanismi di tracciabilità circa i flussi documentali;
2) incaricare e gestire gli addetti al trattamento secondo criteri di trasparenza, in coerenza con i valori etici e nel rispetto delle leggi e dei regolamenti esistenti;
3) informare e istruire i propri collaboratori sulle modalità di condotta operativa da adottare nelle procedure che prevedono il trattamento dei dati, trasferendo conoscenza della norma e consapevolezza delle situazioni a rischio reato.

Inoltre, secondo quanto previsto dalle Linee Guida AGiD, Il RGD, d'intesa con il Responsabile della Conservazione e il Responsabile per la Transizione Digitale (art.17 del CAD), e acquisito il parere del Responsabile della Protezione dei Dati Personali, (artt. 37 "Designazione del responsabile della protezione dei dati" e 39 "Compiti del responsabile della protezione dei dati" del Regolamento UE 679/2016), predispone:

- il MGD relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso ai documenti informatici nel rispetto della normativa in materia di trattamenti dei dati personali ed in coerenza con quanto previsto nel manuale di conservazione.

Pertanto, il RGD è responsabile della redazione e dell'aggiornamento del MGD e, tutte le strutture organizzative dell'ISS, sono tenute a fornire tempestive indicazioni in merito a qualsivoglia evento suscettibile di incidere sull'operatività del presente MGD, in modo tale da adottare gli eventuali interventi correttivi e/o integrativi ritenuti necessari.

1.9. Profili di abilitazione alle informazioni del sistema di gestione documentale

Nell'ambito dell'ISS, il sistema di Gestione Documentale permette l'assegnazione differenziata dei seguenti profili:

- Responsabile della Gestione Documentale o RGD (funzioni decisionali e di delega);
- Amministratore di sistema (funzioni gestionali a seguito della decisione del RGD);
- Utente di Protocollo o Protocollatore (funzioni operative);
- Consultatore (funzioni di visualizzazione).

Inoltre, è garantita la protezione dei dati personali secondo quanto già descritto.
L'Ufficio I-Affari Generali riceve, dai vari Dirigenti, richiesta scritta (anche tramite e-mail o sistema di supporto) di abilitazione per ciascun profilo utente, concordando, caso per caso, le tipologie di abilitazione.
Il profilo di ogni utente è generato mediante la personalizzazione dei modelli predefiniti elencati sopra.

1.10. Accreditamento all'IPA e casella di posta elettronica certificata dell'Ufficio Protocollo

L'ISS, in osservanza agli adempimenti normativamente previsti, si è accreditato presso l'Indice delle Pubbliche Amministrazioni (IPA), fornendo le informazioni che individuano l'amministrazione e l'articolazione dell'AOO.
L'IPA, quale Archivio ufficiale degli Enti Pubblici e dei Gestori di pubblici servizi, è accessibile tramite il relativo sito internet da parte di tutti i soggetti pubblici o privati interessati. L'amministrazione comunica tempestivamente all'IPA informazioni dettagliate in merito alla propria struttura organizzativa, alle competenze dei singoli uffici ed ai servizi offerti, nonché rende nota ogni successiva modifica delle proprie credenziali di riferimento e la data in cui la stessa sarà operativa, garantendo l'affidabilità del proprio indirizzo di posta elettronica; con la stessa tempestività l'amministrazione comunica la soppressione, ovvero la creazione di una AOO.
La casella di posta elettronica certificata istituzionale dell'AAPC dell'ISS, pubblicata sull'IPA, è la seguente: **protocollo.centrale@pec.iss.it**.
La medesima casella è accessibile, per la ricezione e l'inoltro dei documenti, al solo AAPC, mentre i relativi interventi di manutenzione e gestione tecnica sono demandati all'*Area Risorse strumentali e Tecnologie informatiche,* anch'essa facente parte dell'*Ufficio I-Affari Generali*.

1.11. Altre caselle di posta elettronica istituzionale certificata e non certificata

In osservanza a quanto previsto dalla normativa vigente, l'ISS dota gli Uffici amministrativi e le Strutture scientifiche di una propria casella di posta elettronica istituzionale certificata, mentre tutti i dipendenti sono dotati di una casella di posta elettronica istituzionale, e, solo qualora le attività svolte dai singoli lo richiedano, di una casella di posta elettronica certificata.
Gli indirizzi di posta elettronica degli Uffici amministrativi e delle Strutture scientifiche dell'ISS sono pubblicati sul sito Internet dell'Ente, sezione "Amministrazione Trasparente", in adempimento a quanto statuito dal D. Lgs. 33/2013 ss.mm.ii.

1.12. Prescrizioni conseguenti all'avvio del sistema di protocollo informatico e cessazione dei cosiddetti "protocolli interni"

Con il sistema informatico di gestione dei flussi documentali sono divenute pienamente efficaci le disposizioni che vietano l'uso dei cosiddetti protocolli interni (cioè, di Direzione/Ufficio/Dipartimento/Centro ecc..), i quali, tutt'al più, potranno avere la funzione di mere "rubriche interne" atte a tenere memoria della documentazione afferente alla singola UO, ovvero di altri sistemi di registrazione dei documenti diversi dal protocollo unico dell'AOO.
In particolare, il sistema di protocollo informatico si uniforma al rispetto delle prescrizioni di cui al successivo paragrafo 2.2.
È compito del RGD effettuare, laddove ritenuto necessario, eventuali controlli a campione sulla congruità delle registrazioni, sulla corretta sequenza della catena documentale e sull'utilizzo di un solo registro informatico.

1.13 Gestione della sicurezza informatica

L'infrastruttura informatica a supporto della gestione documentale dell'ISS eroga servizi in conformità ai controlli di sicurezza previsti dalla normativa ISO 27001:2024. Il 20 dicembre 2024, l'ISS ha ottenuto la certificazione ISO 27001 (certificato CSQA n.83998 del 20/12/2024). Questo ha comportato l'implementazione di un Sistema di Gestione per la Sicurezza delle Informazioni che disciplina la gestione in sicurezza di *Progettazione, implementazione e conduzione di reti informatiche, infrastrutture IT, sistemi di sicurezza informatica ed erogazione di servizi di esercizio, sviluppo e manutenzione delle componenti software e sistemi ICT a servizio dell'attività scientifica e amministrativa dell'Istituto Superiore di Sanità*. L'implementazione del sistema di gestione ha altresì comportato l'adozione di specifiche misure rivolte alla gestione della business continuity e del disaster recovery, descritte in apposite procedure operative. Le misure di sicurezza adottate per la gestione documentale in ISS discendono perciò dall'adozione dei controlli implementati dal Sistema di Gestione ISO 27001 nonché dall'analisi del rischio relativa alle specifiche attività svolta in collaborazione con la Struttura di Supporto del DPO ISS.

CAPITOLO II

2. ELEMENTI CARATTERIZZANTI IL PROTOCOLLO INFORMATICO

2.1. Natura giuridica del Protocollo informatico

Il registro del protocollo, in conformità a consolidata giurisprudenza, è atto pubblico di fede privilegiata, idoneo a certificare la veridicità delle informazioni connesse all'elenco dei protocolli registrati nell'arco di uno stesso giorno.
Per mezzo del Registro di protocollo, il pubblico ufficiale attesta l'avvenuta ricezione ovvero trasmissione di un documento, la relativa data e la numerazione progressiva che allo stesso viene attribuita, svolgendo, in tal modo, un'operazione unica e contestuale avente la natura di atto pubblico; la documentazione non registrata dall'Ufficio Protocollo, quindi, viene considerata giuridicamente inesistente presso l'ISS.

2.2. Unicità del protocollo informatico

Nell'ambito dell'ISS, il registro di protocollo è unico ed è gestito dall'AAPC, incardinata nell'Ufficio I - Affari Generali.
Il registro di protocollo è generato automaticamente dal sistema di protocollo informatico che attribuisce a ciascun documento registrato il numero e la data di protocollazione.
Ai sensi dell'art. 57 del DPR 445/2000, il numero di protocollo è costituito da almeno sette cifre numeriche. La numerazione delle registrazioni di protocollo è unica e progressiva, la stessa inizia il 1^ gennaio dal numero 0000001 e si conclude il 31 dicembre di ogni anno. Ogni numero di protocollo si riferisce esclusivamente ad un univoco documento; non è, pertanto, consentita l'identificazione dei documenti mediante l'assegnazione manuale ovvero informatica di numeri di protocollo che il sistema ha già attribuito ad altri documenti, ancorché collegati tra loro.
A seguito dell'introduzione del protocollo unico, inoltre, per garantire la corretta classificazione ed organizzazione dei documenti, viene adottato un unico Titolario di classificazione

2.3. Unicità, immodificabilità e conservazione del protocollo informatico

Al fine di garantire l'immodificabilità del contenuto delle registrazioni di protocollo, si genera quotidianamente, mediante produzione automatica, il registro giornaliero di protocollo, definito come il 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 di gestione informatica dei documenti.
Le regole sulla formazione dei registri e repertori informatici sono contenute nel TUDA che dispone la registrazione informatica dei documenti, prodotti e acquisiti dalle Pubbliche Amministrazioni, al fine della loro identificazione univoca.
Il registro giornaliero di protocollo, quindi, è il documento che traccia, in modo ordinato e progressivo, le operazioni di registrazione, protocollazione ed annullamento effettuate nell'arco della giornata a cui si riferisce.
Infatti, la segnatura di protocollo è l'associazione, ai documenti informatici, in forma permanente e non modificabile, di informazioni riguardanti i documenti stessi, in ingresso e in uscita al sistema di protocollo, utile alla sua identificazione univoca e certa.
Oltre ad assicurare l'immodificabilità ed integrità nel tempo del Registro, è necessario assicurare il rispetto delle disposizioni in materia di sicurezza predisposte dall'AgID e dagli altri organismi preposti e delle disposizioni in materia di protezione dei dati personali.
In particolare, il sistema di protocollo informatico deve garantire:

a) l'univoca identificazione ed autenticazione degli utenti;
b) la garanzia di accesso alle risorse esclusivamente agli utenti abilitati e/o a gruppi di utenti secondo la definizione di appositi profili;
c) il tracciamento permanente di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore.
Il registro giornaliero di protocollo è trasmesso entro la giornata lavorativa successiva al sistema di conservazione, garantendone l'immodificabilità del contenuto.

2.4. Contenuti minimi del Registro giornaliero di protocollo

Il registro giornaliero di protocollo deve contenere le informazioni minime previste dal TUDA e dalle Linee Guida AGiD.
In particolare, con riferimento a ciascun documento ricevuto o spedito, la registrazione di protocollo richiede la memorizzazione delle seguenti informazioni:

- il numero di protocollo del documento, generato automaticamente dal sistema e registrato in forma non modificabile;
- la data di registrazione di protocollo, assegnata automaticamente dal sistema e registrata in forma non modificabile;
- il mittente ovvero il destinatario per i documenti ricevuti od inviati, registrati in forma non modificabile;
- l'oggetto del documento, registrato in forma non modificabile;
- la data ed il protocollo del documento ricevuto, se disponibili;
- l'impronta del documento informatico, se trasmesso per via telematica, costituita dalla sequenza di simboli binari in grado di identificarne univocamente il contenuto, registrata in forma non modificabile;
- l'indicazione del registro nell'ambito del quale è stata effettuata la registrazione.

CAPITOLO III

3. IL DOCUMENTO

3.1. Documento amministrativo

Per documento amministrativo si intende, ai sensi dell'art. 1, co. 1, lett. a) del DPR n. 445/2000 "*ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa*".
Il documento amministrativo è, in altri termini, ogni rappresentazione grafica, fotocinematografica, elettromagnetica o di qualunque altra specie del contenuto di atti, anche interni, detenuti da una pubblica amministrazione e concernenti attività di pubblico interesse, indipendentemente dalla natura pubblicistica o privatistica della loro disciplina sostanziale.
A seconda del supporto che lo contiene, il documento amministrativo può essere analogico ovvero informatico.

3.2. Documento informatico

Per documento informatico si intende, ai sensi dell'art. 1, co. 1, lett. b), del DPR n. 445/2000 e dell'art. 1, co. 1, lett. p) del CAD "*la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti*".
Sul piano generale, il CAD sancisce la validità e la rilevanza agli effetti di legge del documento informatico da chiunque formato, della sua memorizzazione su supporto informatico e della trasmissione con strumenti telematici conformi alle regole tecniche. Una volta rispettate le regole tecniche, il documento informatico realizzato, memorizzato e trasmesso con strumenti telematici ha identica validità, ad ogni effetto di legge, del documento cartaceo e deve essere accettato da qualsiasi soggetto pubblico o privato.
In particolare, le caratteristiche di integrità ed immodificabilità del documento informatico sono assicurate, fra le altre operazioni, dalla sottoscrizione dello stesso con firma digitale, definita quale "particolare tipo di firma qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare, tramite la chiave privata, e ad un soggetto terzo, 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" (CAD, art. 1, co. 1, lett. s).
Per quanto riguarda l'individuazione dei formati utilizzati per la formazione del documento informatico si fa rinvio a quanto previsto nell'Allegato 2 delle Linee Guida AgID contenente "Formati di file e riversamento".

3.3. Documento analogico

Per documento analogico si intende la "rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti" (CAD, art. 1, lett. p - bis).
Il documento analogico può essere prodotto sia con strumenti analogici (es. a mano) che con strumenti informatici (es. lettera scritta con software di videoscrittura). Il supporto del documento è un oggetto materiale; l'originale dell'atto, infatti, è cartaceo e dotato di firma autografa.

3.4. Documenti prodotti dall'ISS

L'ISS, in osservanza all'art. 40, co. 1, del CAD, forma gli originali dei propri documenti con mezzi informatici.

Qualsivoglia documento, sia esso analogico che informatico, deve essere corredato delle firme (autografe ovvero digitali) necessarie alla perfezione giuridica dello stesso, le quali devono essere apposte prima della sua protocollazione.
Ciascun documento prodotto dall'Istituto viene univocamente identificato a mezzo di un solo protocollo, pur potendo fare riferimento a diversi procedimenti o fascicoli.

3.5. Documenti in ingresso

I documenti in ingresso sono tutti gli atti aventi rilevanza giuridico probatoria prodotti da soggetti terzi ed acquisiti dall'ISS nell'esercizio delle proprie funzioni istituzionali.
I documenti analogici trasmessi da soggetti esterni all'Amministrazione sono recapitati a mezzo posta convenzionale e/o raccomandata, telegramma, a mezzo corriere, ovvero con consegna diretta da parte dell'interessato o persona dallo stesso delegata.
I documenti informatici sono recapitati a mezzo posta elettronica convenzionale o certificata, a mezzo di supporto rimovibile (quale, ad esempio, CD ROM, DVD, pen drive, ecc.) consegnato direttamente o inviato per posta o tramite corriere.

3.6. Documenti in uscita

I documenti in uscita sono tutti gli atti aventi rilevanza giuridico probatoria prodotti dal personale dell'ISS nell'esercizio delle proprie funzioni istituzionali e trasmessi a soggetti esterni.
I documenti analogici possono essere trasmessi a mezzo di posta convenzionale e/o raccomandata, a mezzo di corriere, telegramma, ovvero tramite consegna diretta al destinatario.
I documenti informatici sono, di norma, trasmessi ai destinatari a mezzo della posta elettronica certificata ovvero mediante e-mail istituzionali. In altri casi, il documento informatico può essere riversato su supporto rimovibile non modificabile ed inviato / consegnato al destinatario.

3.7. Documenti interni

I documenti interni sono tutti gli atti prodotti e destinati alla circolazione all'interno dell'ISS; i medesimi possono avere natura prevalentemente informativa, ovvero giuridico-probatoria.
I documenti interni di natura meramente informativa (quali, a titolo esemplificativo, comunicazioni interne inerenti a luoghi e date di riunioni scambiate tra uffici, richieste di materiale di consumo ovvero di interventi di assistenza informatica ecc..) non sono normalmente soggetti a protocollazione e di regola, lo scambio di tali documenti avviene a mezzo della posta elettronica.
I documenti interni di natura prevalentemente giuridico-probatoria, ossia tutti gli atti redatti dal personale dell'ISS nell'esercizio delle proprie funzioni, volti a documentare le attività istruttorie di competenza (quali, a titolo esemplificativo, circolari e/o relazioni istruttorie, pareri o verbali di riunioni svolte presso gli Uffici), devono essere protocollati.
Nei casi in cui il documento interno di natura giuridico–probatoria sia di tipo analogico, lo scambio nell'ambito dell'Amministrazione può avvenire con i mezzi tradizionali: il documento viene prodotto con strumenti informatici, stampato e sottoscritto in forma autografa e successivamente protocollato, per poi essere consegnato direttamente al destinatario. Qualora, invece, il documento interno di natura giuridico–probatoria sia di tipo digitale, lo stesso, dopo l'apposizione di eventuale firma elettronica grafica, avanzata o qualificata ed essere stato protocollato, sarà di norma trasmesso tramite e-mail o supporto informatico.

3.8. Duplicato, copia ed estratto di documenti informatici

Il duplicato del documento informatico è un documento prodotto mediante idoneo processo o strumento che assicuri che il documento informatico, ottenuto sullo stesso sistema di

memorizzazione o su un sistema diverso, contenga la stessa sequenza binaria del documento informatico di origine da cui è tratto.
La copia o estratto di un documento informatico è un documento informatico che può mutare il formato del documento originario o che muta il supporto del documento originario informatico. (ad es., il salvataggio di un file in un formato differente: da .doc a .pdf, oppure da .doc a .ods).
Le copie del documento informatico hanno la stessa efficacia probatoria dell'originale da cui sono tratte se la loro conformità è attestata da un pubblico ufficiale autorizzato o se la conformità non è espressamente disconosciuta, fermo l'obbligo di conservazione dell'originale informatico (c.3 art. 23-bis e art.71 del CAD).
Pertanto mentre le copie di documenti informatici limitano a mantenere il contenuto dei documenti originali (ma non il loro formato), i duplicati informatici non necessitano di attestazione di conformità all'originale da parte di un notaio o di un pubblico ufficiale, stante la loro perfetta corrispondenza nel numero, nella sequenza dei valori binari e hanno il medesimo valore giuridico del documento informatico da cui sono tratti qualora prodotti mediante processi e strumenti che assicurino la predetta sequenza.

3.9. Metadati

Secondo la definizione dell'ISO (International Organization for Standardization) i metadati sono "dati che descrivono e definiscono altri dati in un determinato contesto".
In ambito di gestione documentale informatizzata il metadato descrive il contenuto, la struttura e l'ambito in cui s'inquadra un documento informatico, per la sua gestione, conservazione e archiviazione.
Gli obiettivi dei metadati sono:

- garantire l'identificazione permanente dei singoli oggetti informativi;
- garantire l'identificativo univoco (numero di protocollo, data, autore, ecc.);
- garantire l'identificazione permanente delle relazioni tra gli oggetti informativi (ad es. indici di classificazione e fascicolatura);
- conservare le informazioni che supportano l'intellegibilità degli oggetti informativi (ad es. procedimento amministrativo cui il documento è connesso).

CAPITOLO IV

4. GESTIONE DELLA CORRISPONDENZA IN ENTRATA

4.1. Regole generali di assegnazione e smistamento dei documenti

Attraverso l'attività di assegnazione di un documento per il tramite dell'applicativo informatico in uso, l'AAPC individua l'Ufficio/Struttura competente alla trattazione dello stesso e, quindi, del relativo procedimento amministrativo.
L'assegnazione può essere effettuata per competenza o per conoscenza e può essere estesa a tutti i soggetti ritenuti interessati alla trattazione del documento, onde consentire la massima condivisione delle informazioni.
A seguito dell'assegnazione, il Responsabile dell'Unità competente - che provvede alla presa in carico del documento e, in applicazione delle vigenti disposizioni organizzative, all'eventuale sub-assegnazione al responsabile dell'istruttoria - verifica la corretta classificazione del documento, eventualmente segnalando all'AAPC la necessità di provvedere a correzioni, inserisce lo stesso in apposito fascicolo elettronico, nonché provvede alla lavorazione ovvero all'archiviazione del documento.
I termini per la definizione del procedimento amministrativo che prende avvio da un determinato documento decorrono, di norma, dalla data di protocollazione.
Il sistema di gestione informatica dei documenti memorizza tutti i passaggi e le eventuali modifiche, conservando, per ciascuno di essi, l'identificativo dell'utente che effettua l'operazione, la data e l'ora di esecuzione.

4.2. Ricezione di documenti analogici

I documenti analogici che pervengono quotidianamente a mezzo posta sono sottoposti dal personale dell'AAPC ad una preliminare verifica in merito alla correttezza dell'indirizzo e del soggetto destinatario sugli stessi apposti.
La busta viene allegata al documento al fine di assicurare la piena visione dei timbri postali.
I documenti ricevuti via telegramma, per ciò che concerne la registrazione di protocollo, sono gestiti come un documento cartaceo.
Dopo aver proceduto all'assegnazione dei documenti all'Ufficio/Struttura di competenza, il personale provvede alla loro scansione (con acquisizione del relativo file nel sistema), registrazione, segnatura e classificazione.
In osservanza all'art. 53, c. 5, del DPR n. 445/2000, sono esclusi dalla registrazione di protocollo i seguenti documenti: gazzette ufficiali, bollettini ufficiali e notiziari della pubblica amministrazione, note di ricezione delle circolari ed altre disposizioni, materiali statistici, atti preparatori interni, giornali, riviste, libri, materiali pubblicitari, inviti.

4.3. Ricezione di documenti informatici

Di norma, la ricezione dei documenti informatici è assicurata tramite la casella di posta elettronica certificata istituzionale (*protocollo.centrale@pec.iss.it*).
Il personale dell'AAPC controlla quotidianamente i messaggi pervenuti nella casella di posta istituzionale e, previa verifica della leggibilità ed integrità del messaggio, procede all'assegnazione, registrazione, segnatura e classificazione dei relativi documenti.
Nel caso in cui il messaggio pervenuto tramite la suddetta posta elettronica sia illeggibile od incompleto, il personale deve, di norma, segnalare la circostanza al mittente, indicando che lo stesso non verrà sottoposto a protocollazione.

I documenti informatici in arrivo possono essere dotati di firma o meno.
In particolare, la firma digitale di cui all'art. 1 c.1, lett. n) del DPR n. 445/2000 ed all'art. 1, c.1, lettera s) del CAD, costituisce l'unico strumento che soddisfa i requisiti di sicurezza dell'identificabilità del sottoscrittore, nonché dell'integrità ed immodificabilità del documento.
La firma digitale, quale equivalente elettronico della tradizionale firma autografa su carta, è associata stabilmente al documento elettronico sulla quale è apposta e ne attesta con certezza l'integrità, l'autenticità, la non ripudiabilità.
Per quanto attiene all'efficacia probatoria del documento informatico sottoscritto, si ricorda che, ai sensi dell'art. 20, c. 1 bis, del CAD, "*Il documento informatico soddisfa il requisito della forma scritta e ha l'efficacia prevista dall'articolo 2702 del Codice civile quando vi è apposta una firma digitale, altro tipo di firma elettronica qualificata o una firma elettronica avanzata o, comunque, è formato, previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dall'AgID ai sensi dell'articolo 71 con modalità tali da garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore. In tutti gli altri casi, l'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, in relazione alle caratteristiche di sicurezza, integrità e immodificabilità. La data e l'ora di formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle Linee guida.*".

4.4. Errata ricezione di documenti analogici

Qualora all'AAPC, pervengano erroneamente documenti analogici indirizzati ad altri Enti, le relative buste e/o contenitori devono essere restituiti. Nel caso in cui la busta venga aperta per errore, il plico viene immediatamente repentinamente chiuso e imbustato per essere trasmesso alla AOO destinataria.

4.5. Errata ricezione di documenti informatici

Nel caso in cui pervengano, sulla casella di posta elettronica certificata istituzionale dell'ISS, messaggi dal cui contenuto si rileva che i medesimi sono stati erroneamente ricevuti, l'operatore dell'AAPC rispedisce il messaggio al mittente, senza protocollarlo, apponendovi una dicitura del tipo "messaggio pervenuto per errore, non di competenza di questa AOO".

4.6. Rilascio di ricevute attestanti la ricezione di documenti analogici

Qualora un documento cartaceo non soggetto a protocollazione sia consegnato direttamente all'AAPC e sia richiesto il rilascio di una ricevuta attestante l'avvenuta consegna, l'operatore di protocollo che lo riceve è autorizzato a fotocopiare gratuitamente la prima pagina del documento e ad apporvi il timbro dell'ISS recante la data e l'ora d'arrivo, nonché ad apporre la sigla dell'operatore incaricato.
L'apposizione del timbro dell'Istituto con la data e l'ora d'arrivo e la sigla dell'operatore sulla copia, tuttavia, non è idonea ad attestare, con valenza giuridico-probatoria, l'avvenuta ricezione di un documento soggetto a protocollazione.
Infatti, nel caso siano ricevuti documenti analogici soggetti a protocollazione e sia richiesto il rilascio di una ricevuta attestante l'avvenuta consegna, l'operatore che riceve il documento dovrà rilasciare idonea ricevuta, ovvero fotocopiare gratuitamente la pagina del documento sulla quale è stata apposta la segnatura di protocollo.

4.7. Rilascio di ricevute attestanti la ricezione di documenti informatici

Nel caso di ricezione di documenti informatici mediante la casella di posta elettronica certificata, la notifica al mittente dell'avvenuto recapito del messaggio è assicurata dagli specifici standard del servizio di posta elettronica certificata dell'AOO.

4.8. Termini per la registrazione di protocollo

Le registrazioni di protocollo dei documenti ricevuti sono effettuate in giornata e, comunque, non oltre due giorni lavorativi dal ricevimento, nel caso di oggettive impossibilità.

4.9. Differimento dei termini di registrazione

Nel caso di eccezionale carico di lavoro, che non permetta di evadere la corrispondenza ricevuta nei tempi sopra indicati e qualora dalla mancata registrazione di protocollo del documento nella medesima giornata lavorativa di ricezione possa risultare leso un diritto di terzi, con motivato provvedimento del RDG, è autorizzato l'uso del protocollo differito.
In particolare, il protocollo differito consiste nell'adozione di un provvedimento con il quale vengono individuati i documenti da ammettere alla registrazione differita, le cause ed il termine entro il quale la registrazione di protocollo deve essere comunque effettuata.
Il protocollo differito si applica solo ai documenti in arrivo e per tipologie omogenee che il RDG deve descrivere nel provvedimento.

4.10. Registrazione e segnatura dei documenti in entrata

Su ogni documento ricevuto dall'ISS è effettuata una registrazione di protocollo attraverso il sistema di gestione del protocollo informatico.
In particolare, come già detto, ciascuna registrazione di protocollo contiene, ai sensi dell'art. 53 del DPR 445/2000, i seguenti dati obbligatori in forma non modificabile:
a) il numero di protocollo, generato automaticamente dal sistema e registrato in forma non modificabile;
b) la data di registrazione di protocollo, assegnata automaticamente dal sistema e registrata in forma non modificabile;
c) il mittente per i documenti ricevuti o, in alternativa, il destinatario per i documenti spediti, registrati in forma non modificabile;
d) l'oggetto del documento, registrato in forma non modificabile;
e) la data ed il numero di protocollo del documento ricevuto, se disponibili;
f) l'impronta del documento informatico, se trasmesso per via telematica, costituita dalla sequenza di simboli binari in grado di identificarne univocamente il contenuto, registrata in forma non modificabile.
L'operazione di segnatura di protocollo è effettuata contemporaneamente all'operazione di registrazione ed avviene attraverso l'apposizione su di esso di un "segno" grafico (realizzato mediante apposizione di timbro grafico sul documento digitale) sul quale vengono riportate le seguenti informazioni relative alla registrazione di protocollo:

- codice identificativo o nome per esteso dell'ISS;
- classificazione, data e numero di protocollo del documento.

La segnatura di protocollo deve essere effettuata sulla prima pagina del documento.
I documenti pervenuti alla casella di posta elettronica istituzionale, una volta registrati, sono sottoposti a segnatura automaticamente dal sistema di protocollo informatico.

4.11. Diritto di accesso e tutela dei dati personali

L'ISS nella gestione dei flussi documentali di propria competenza, si uniforma alle norme vigenti in materia di diritto di accesso e di protezione dei dati personali.
Le modalità di esercizio del diritto di accesso ai documenti amministrativi dell'ISS nelle due forme dell'accesso documentale (ex lege n. 241/1990 e ss.mm.ii.) e dell'accesso civico (ex D. Lgs n. 33/2013 e ss.mm.ii.) sono disciplinate, rispettivamente, dal *Regolamento in materia di diritto di accesso ai documenti amministrativi dell'ISS* e dal *Regolamento in materia di accesso civico "semplice e generalizzato"*, consultabili nella specifica sezione di Amministrazione Trasparente dell'Ente.
L'ISS, quale soggetto titolare del trattamento di dati (comuni, sensibili e/o giudiziari) contenuti nella documentazione di propria competenza, dà attuazione alle disposizioni di cui al Regolamento UE 2016/679 ed al D. Lgs 196/2003 e ss.mm.ii.
In particolare, il personale dell'AAPC, preposto all'apertura ed alla registrazione della corrispondenza, deve essere regolarmente autorizzato al trattamento dei dati personali.
Invero, il personale tutto, nell'esercizio delle proprie funzioni, è tenuto all'osservanza del segreto d'ufficio, nonché dei doveri e degli obblighi previsti dalla normativa di riferimento, a non trarre benefici personali ed a non nuocere a terzi ed all'immagine dell'Ente in conseguenza della conoscenza di particolari circostanze, dati ed informazioni desumibili dai documenti di propria pertinenza.
Qualora la corrispondenza riservata personale, in forma cartacea, venga recapitata per errore ad un diverso Ufficio/Struttura, a tutela dei dati personali e /o sensibili eventualmente contenuti, il relativo plico va restituito integro (non vanno aperte le buste o i contenitori), nella stessa giornata, all'AAPC. Detta Area provvederà, quindi, a fare pervenire la corrispondenza al destinatario effettivo senza procedere alla protocollazione.
Alcune strutture dell'Ente, su richiesta e previa autorizzazione del RGD, possono dotarsi di un protocollo riservato per l'invio e la ricezione di documentazione per la quale va tutelata la riservatezza dei dati personali.

CAPITOLO V

5. GESTIONE DELLA CORRISPONDENZA IN USCITA

5.1. Regole generali

I documenti in uscita sono quelli prodotti dagli Uffici dell'ISS nell'esercizio delle proprie funzioni istituzionali, aventi rilevanza giuridico-probatoria e destinati ad essere trasmessi a soggetti terzi.
I documenti in partenza verso destinatari esterni all'Ente sono sottoposti, da parte del personale dell'AAPC, alle procedure di registrazione e segnatura, classificati secondo il Titolario di Classificazione ed allegati in formato pdf/a ai dati di registrazione di protocollo.
Tali operazioni sono, allo stato attuale, effettuate centralmente dalla AAPC, ma eventuali abilitazioni ad eseguire le medesime attività da parte delle segreterie delle singole UO possono essere stabilite successivamente in conformità alle valutazioni del caso.
Ciascuna registrazione di protocollo in uscita deve contenere, almeno, i seguenti dati obbligatori in forma non modificabile:

- il numero di protocollo, generato automaticamente dal sistema;
- la data di registrazione di protocollo, assegnata automaticamente dal sistema;
- il mittente che ha prodotto il documento;
- il destinatario del documento;
- l'oggetto del documento.

I documenti in uscita sono solamente quelli informatici, che vengono protocollati direttamente dagli utenti autorizzati delle strutture dell'Ente ovvero, laddove questi ultimi non possano provvedere, dagli operatori dell'AAPC.
L'operatore di protocollo, dopo aver provveduto alla registrazione del documento, si occupa a livello centralizzato della relativa trasmissione attraverso la casella di posta elettronica certificata istituzionale (*protocollo.centrale@pec.iss.it*).
Solo la trasmissione dalla casella di pec istituzionale ad una casella pec del destinatario costituisce evidenza giuridico-probatoria dell'invio e della consegna del messaggio (art. 47 CAD).
Al fine di garantire la riservatezza dei dati di cui agli articoli 9 e 10 GDPR (categorie particolari di dati personali e dati personali relativi a condanne penali e reati) eventualmente contenuti in seno alla documentazione trasmessa, l'art. 46 del CAD dispone che i documenti informatici trasmessi ad altre pubbliche amministrazioni per via telematica possono contenere soltanto i dati consentiti da legge o da regolamento e indispensabili per il perseguimento delle finalità per le quali sono acquisite.
Le ricevute digitali del sistema di posta elettronica certificata utilizzato per lo scambio dei documenti digitali sono trasmesse dall'AAPC alle UO mittenti e da quest'ultime conservate all'interno dei relativi fascicoli.
Nei casi in cui il destinatario sia sprovvisto di un indirizzo di posta elettronica certificata, il documento digitale può essere prodotto in formato cartaceo (sebbene debba essere sempre sottoposto a scansione in fase di protocollazione) e conseguentemente trattato come fosse un documento analogico.
Un originale del documento trasmesso deve essere conservato dal soggetto che lo ha formato, il quale provvede, altresì, ad inserirlo nel fascicolo relativo al procedimento cui si riferisce e/o ad archiviarlo.

CAPITOLO VI

6. GESTIONE DI CATEGORIE PARTICOLARE DI CORRISPONDENZA

6.1. Corrispondenza riservata

Per i procedimenti amministrativi o gli affari per i quali si renda necessaria la riservatezza delle informazioni, è prevista una specifica funzionalità del sistema applicativo in uso, che consente la gestione di un protocollo riservato, non accessibile alla consultazione da parte dei soggetti non espressamente abilitati.
I documenti soggetti a questa particolare procedura possono essere i seguenti:

- atti dei procedimenti amministrativi in relazione ai quali sussistano particolari esigenze di protezione della riservatezza di terzi, persone, gruppi, imprese ed associazioni e dalla cui contestuale pubblicità possa derivare pregiudizio a terzi o al buon andamento dell'attività amministrativa;
- atti contenenti informazioni classificate o coperte da segreto di Stato;
- documenti relativi a vicende di persone o a fatti privati o particolari;
- documenti di carattere politico e di indirizzo che, se resi di pubblico dominio, possono ostacolare il raggiungimento degli obiettivi prefissati;
- le tipologie di documenti individuati dall'art. 24 della legge 7 agosto 1990 n. 241;
- documenti che contengano dati personali, comuni, relativi alle particolari categorie e relativi a condanne penali e reati, come definiti dalla vigente normativa in materia di protezione dei dati personali.

La selezione della casella "riservato" rende la protocollazione riservata e visibile ai soli utenti abilitati.
In particolare, su indicazione del Presidente e/o del Direttore Generale e conseguente autorizzazione del RDG, l'operatore di protocollo, all'atto della registrazione del documento, deve selezionare l'apposita casella "riservato" ed il nominativo dell'assegnatario, per rendere il documento visibile esclusivamente dal protocollatore e dal destinatario.
La procedura di cui sopra consente di eseguire sul documento c.d. riservato tutte le operazioni (quali la registrazione, la segnatura, la classificazione e la fascicolazione) adottate per gli altri documenti e procedimenti amministrativi.
In caso di documento analogico, va eseguita la scansione ai fini della conservazione dello stesso in formato pdf/a.
Nell'ipotesi di riservatezza temporanea delle informazioni è necessario indicare, contestualmente alla registrazione di protocollo, anche la data a partire dalla quale le informazioni temporaneamente riservate diverranno soggette all'accesso ordinariamente previsto.

6.2. Documenti indirizzati nominalmente al personale dell'Istituto

La posta indirizzata nominalmente al personale dell'Istituto è regolarmente aperta e registrata al protocollo, a meno che sulla busta non sia riportata la dicitura "personale" / "riservata personale", ovvero espressione equivalente. In questo caso, la corrispondenza viene consegnata in busta chiusa al destinatario, il quale, qualora reputi che i documenti acquisiti debbano essere comunque protocollati, provvede a trasmetterli all'AAPC ai fini delle ordinarie procedure di registrazione di protocollo.

6.3. Documenti anonimi o privi di sottoscrizione

I documenti anonimi analogici sono sottoposti dal protocollatore all'attenzione del RGD per l'opportuna procedura e le valutazioni di competenza.

6.4. Documenti con più destinatari

I documenti recanti un unico oggetto, ma indirizzati ad una pluralità di destinatari (ad es. le disposizioni generali, gli ordini di servizio e tutte le altre comunicazioni interne che abbiano più destinatari), si registrano con un solo numero di protocollo generale; i destinatari, se in numero consistente, sono contenuti in appositi elenchi allegati al documento.
Le stesse disposizioni si applicano per i documenti in partenza con più destinatari.

6.5. Protocollazione di un numero consistente di documenti

Qualora si presenti la necessità di protocollare un numero consistente di documenti, sia in ingresso che in uscita, l'UO interessata deve darne comunicazione all'AAPC con congruo anticipo (almeno due giorni lavorativi), al fine di concordare tempi e modi di protocollazione e di spedizione.

6.6. Protocolli urgenti

Il RGD può disporre la protocollazione immediata di documenti urgenti, nel caso in cui il carattere d'impellenza emerga dal contenuto dei documenti stessi, ovvero sia motivatamente segnalato dai Responsabili delle competenti UO.

6.7. Integrazioni documentarie

In caso di acquisizione all'AAPC di integrazioni documentarie, il personale addetto non è tenuto a verificare la completezza sostanziale della documentazione pervenuta.

CAPITOLO VII

7. FASCICOLAZIONE DEI DOCUMENTI

7.1. Fascicolazione dei documenti

Ogni documento, dopo la registrazione e classificazione centralizzata da parte dell'AAPC, viene di norma inserito, a cura della competente UO, nel fascicolo di riferimento.
Ai sensi dell'art. 52, co. 1, lett. c), del DPR 445/2000 il sistema di protocollo informatico fornisce, tra l'atro, anche "le informazioni sul collegamento esistente tra ciascun documento ricevuto dall'Amministrazione e i documenti dalla stessa formati nell'adozione dei provvedimenti finali".
Il fascicolo informatico è, appunto, lo strumento che consente, all'interno del sistema di protocollo informatico, l'accorpamento dei documenti in base alla loro pertinenza ad un medesimo procedimento.
L'operazione di fascicolazione viene gestita attraverso le funzioni ad essa dedicate nel sistema di protocollo, con possibilità di archiviare i documenti afferenti allo stesso procedimento all'interno di ciascun fascicolo secondo l'ordine cronologico di registrazione.
Poiché il sistema consente esclusivamente la gestione dei documenti protocollati, ove fossero presenti documenti non soggetti a registrazione di protocollo, comunque utili per la ricostruzione del procedimento, il Responsabile del Procedimento deve curarne l'archiviazione per la successiva integrazione del fascicolo.
Quando un nuovo documento viene recapitato all'ISS, l'UO assegnataria stabilisce, con l'ausilio delle funzioni di ricerca del sistema di protocollo informatico, se il documento stesso debba essere collegato ad un procedimento in corso e, pertanto, se debba essere inserito in un fascicolo già esistente, oppure se il documento si riferisce ad un nuovo procedimento, per cui è necessario aprire un nuovo fascicolo.
A seconda delle ipotesi, si procede come segue:

1. Se il documento si ricollega ad un affare o procedimento in corso, l'addetto dell'Ufficio competente:
   - seleziona il relativo fascicolo;
   - collega la registrazione di protocollo del documento al fascicolo selezionato;
2. Se il documento dà avvio ad un nuovo fascicolo, il soggetto preposto:
   - esegue l'operazione di apertura del fascicolo;
   - collega la registrazione di protocollo del documento al nuovo fascicolo aperto.

L'operazione di "apertura" di un nuovo fascicolo comprende la registrazione di alcune informazioni essenziali:

- oggetto del fascicolo;
- nominativo del Responsabile del Procedimento;
- numero del fascicolo (assegnato automaticamente dal sistema di protocollo informatico);
- data di apertura del fascicolo;
- collocazione fisica dei documenti cartacei di cui si compone;
- data di chiusura del fascicolo (il fascicolo viene chiuso al termine del procedimento amministrativo; la data di chiusura si riferisce a quella relativa all'ultimo documento prodotto)

CAPITOLO VIII

8. REGISTRO DI EMERGENZA E CHIUSURA REGISTRO DI PROTOCOLLO

8.1. Registro di emergenza

Nel caso di interruzioni del funzionamento del sistema per la gestione del protocollo, per cause tecniche accidentali o programmate, ai sensi dell'art. 63 del DPR 445/2000, le registrazioni di protocollo vengono effettuate su un supporto alternativo, denominato registro di emergenza.
In particolare, il RGD autorizza, con proprio atto, la predisposizione del registro di emergenza in forma cartacea o digitale.
Sul registro di emergenza devono essere riportate la causa, la data e l'ora di inizio dell'interruzione, nonché la data e l'ora di ripristino della piena funzionalità del sistema informatico unico di protocollo e le eventuali annotazioni ritenute utili.
Quando viene ripristinata la piena funzionalità del sistema, l'AAPC provvede alla chiusura del registro di emergenza, annotando sullo stesso, oltre alla data ed ora di chiusura, il numero delle registrazioni effettuate.
Gli operatori dell'AAPC procedono, quindi, alla connessione del registro di emergenza con il protocollo unico, recependo nell'applicativo informatico in uso tutte le registrazioni effettuate sul protocollo di emergenza, continuando la numerazione del protocollo generale raggiunta al momento dell'interruzione del servizio.
Il registro di emergenza viene sostanzialmente a configurarsi come un repertorio del protocollo unico: ad ogni registrazione recuperata dal registro di emergenza sarà attribuito un nuovo numero di protocollo, seguendo senza soluzione di continuità la numerazione del protocollo 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 unico recheranno, pertanto, due numeri: uno del protocollo di emergenza ed uno del protocollo unico.
L'efficacia della registrazione è dunque garantita dal numero attribuito dal registro di emergenza e a quel numero deve farsi riferimento per l'avvio dei termini del procedimento amministrativo; l'efficienza, invece, verrà garantita dall'unicità della catena documentale e dalla normalizzazione dei dati gestionali, comprese la classificazione e la fascicolazione archivistica. Come noto, l'applicativo informatico in uso genera automaticamente, con cadenza quotidiana, il registro giornaliero di protocollo.
Per garantire l'immodificabilità ed integrità nel tempo dell'estrazione statica dei dati del registro giornaliero di protocollo è necessario procedere al trasferimento della stessa nel sistema di conservazione entro la giornata lavorativa successiva.

CAPITOLO IX

9. ORGANIZZAZIONE E GESTIONE DELL'ARCHIVIO

9.1. Archivio e sue partizioni cronologiche

L'archivio è l'insieme dei documenti prodotti e ricevuti dall'amministrazione nell'esercizio delle proprie funzioni ed è, pertanto, il luogo deputato alla idonea custodia degli stessi.
Esso è suddiviso in archivio corrente, di deposito e storico.
Per archivio corrente si intende il complesso dei documenti relativi a procedimenti in corso di istruttoria e di trattazione o, comunque, verso i quali sussista un interesse corrente.
Per archivio di deposito si intende il complesso dei documenti relativi a procedimenti conclusi, ma per i quali la legge prescriva un periodo obbligatorio di custodia o, comunque, verso i quali sussista un interesse sporadico di consultazione.
Per archivio storico si intende il complesso dei documenti relativi a procedimenti conclusi per i quali sussista un interesse storico- istituzionale alla loro custodia permanente.
L'archivio, pur suddiviso nelle tre categorie, è unico.
L'archivio corrente dell'ISS è gestito dai Responsabili delle singole UO, ciascuno con riferimento ai documenti di propria competenza.
Gli elenchi della documentazione da sottoporre alla *Commissione per la sorveglianza degli archivi e lo scarto documentale* sono predisposti a cura del personale dell'AAPC in stretta collaborazione e su indicazione dei Responsabili degli uffici amministrativi e delle strutture scientifiche titolari - per quanto di competenza - della già menzionata documentazione.

9.2. Trasferimento dei documenti dall'archivio corrente a quello di deposito

All'inizio di ciascun anno, di norma, ogni UO individua i fascicoli relativi ai procedimenti conclusi, o comunque non più necessari allo svolgimento delle attività correnti, i quali, unitamente a tutta la documentazione in essi contenuta, vengono trasferiti all'archivio di deposito.
Il trasferimento deve essere effettuato rispettando l'organizzazione che i fascicoli e le serie hanno nell'archivio corrente.
La documentazione relativa alla singola pratica va spedita in una sola copia, in ordine e raggruppata in fascicoli.
Il fascicolo deve contenere solo la documentazione pertinente: corrispondenza protocollata, copie di atti amministrativi, documenti interni rilevanti ai fini del procedimento, e non cataloghi, giornali, depliants vari o corrispondenza personale degli addetti.
Sui pacchi contenenti i documenti da archiviare deve essere segnalato con chiarezza la struttura mittente della spedizione.

9.3. L'archivio storico

L'archivio storico, come precedentemente accennato, contiene le unità archivistiche trasferite, previo scarto, dall'archivio di deposito e considerate meritevoli di custodia permanente per la loro importanza ai fini della ricostruzione delle vicende storiche ed istituzionali del soggetto produttore.
I documenti da detenere sono conservati presso l'archivio storico dell'ISS sotto la vigilanza della Soprintendenza archivistica competente per territorio.
Per i documenti prodotti anteriormente al 1993, quando l'ISS ai sensi del Dlgs n. 267/1993 rivestiva lo status di Amministrazione Centrale dello Stato, rimane tuttora l'obbligo del versamento nell'Archivio Centrale dello Stato.

Successivamente a tale anno, il già menzionato versamento avviene sotto forma di deposito volontario, facoltativo e subordinato al parere della Soprintendenza Archivistica per il Lazio, anche al fine di garantire la continuità storico/archivistica con quanto già in possesso del già menzionato Istituto di conservazione.