Civico Di Cristina Benfratelli
Azienda di Rilievo Nazionale ad Alta Specializzazione

AZIENDA OSPEDALIERA DI RILIEVO NAZIONALE E DI ALTA SPECIALIZZAZIONE

CIVICO — DI CRISTINA — BENFRATELLI

Manuale di Gestione Documentale

Approvato con Delibera n. 251 del 19/02/2025

Emissione del documento

Registro delle versioni

Azione	Data	Nominativo	Funzione
Redazione	17/02/*2025*	Arch. Alba Cristodaro	*Responsabile della gestione documentale*

N°Rev	Delibera di revisione	Modifiche apportate	Osservazioni

Sommario

1 Principi generali

1.1. Premessa

Il presente *Manuale di gestione documentale* è redatto in conformità alle *Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*, emanate dall'Agenzia per l'Italia Digitale (AgID). Queste Linee Guida rappresentano un riferimento normativo e operativo essenziale per garantire la corretta gestione del ciclo di vita dei documenti, dalla loro creazione alla conservazione.

L'obiettivo principale del manuale è quello di definire e descrivere i principi, le procedure e le modalità operative adottate dall'A.R.N.A.S Civico - Di Cristina - Benfratelli (nel seguito, "Arnas") per assicurare:

- la conformità normativa e tecnica nella gestione documentale;
- l'integrità, autenticità, leggibilità e reperibilità dei documenti nel tempo;
- la corretta archiviazione e conservazione secondo criteri di efficienza, sicurezza e trasparenza.

Questo documento si propone di essere uno strumento pratico, in grado di supportare il personale e i responsabili nei processi legati alla gestione dei documenti informatici e analogici, promuovendo l'adozione di buone pratiche e garantendo il rispetto delle normative vigenti.

In particolare, il manuale è strutturato per rispondere alle esigenze operative dell'Ente, delineando:

1. il quadro normativo e regolamentare di riferimento;
2. l'organizzazione interna e le responsabilità connesse alla gestione documentale;
3. le procedure per la gestione del protocollo;
4. le modalità di classificazione, fascicolazione, archiviazione e conservazione dei documenti;

Attraverso la sua applicazione, il Manuale di gestione documentale intende contribuire a un approccio sistematico e organizzato, favorendo la digitalizzazione e la trasformazione digitale dei processi documentali in linea con gli obiettivi di modernizzazione e semplificazione della Pubblica Amministrazione.

1.2. Ambito di applicazione del manuale

Il presente Manuale descrive i principi, le procedure e le modalità operative della Gestione Documentale adottate dall'Arnas.
Esso descrive:

- la formazione, registrazione, classificazione ed archiviazione dei documenti amministrativi, oltre alla gestione dei flussi documentali ed archivistici in relazione ai procedimenti amministrativi delle Aree Organizzative Omogenee (AOO);
- la formazione e gestione di documenti clinici generati dall' Arnas.

Il presente manuale è operativo dalla data di pubblicazione della Delibera di approvazione del Direttore Generale, dalla stessa data tutte le disposizioni in contrasto

con il presente manuale sono da considerarsi decadute. Il presente manuale sarà reso disponibile alla consultazione del pubblico e del personale in servizio presso le AOO tramite la pubblicazione sul sito internet dell'Arnas.

Ad integrazione delle informazioni contenute nel presente Manuale, come da linee guida della Soprintendenza Archivistica della Sicilia, sono allegati i seguenti documenti:

- Delibera di approvazione del Manuale;
- Delibere di nomina dei Responsabili di cui al paragrafo 2.3;
- Piano di conservazione Titolario/massimario di scarto;
- Regolamento per accesso agli atti.

Il presente manuale potrà essere aggiornato a seguito di:

- variazioni normative;
- introduzione di nuove pratiche finalizzate a migliorare l'azione dell'Amministrazione in termini di efficacia, efficienza e trasparenza;
- inadeguatezza delle procedure, rilevata nello svolgimento delle attività correnti.

1.3. Terminologia (Glossario dei termini e degli Acronimi)

Di seguito si riporta la tabella contenente in ordine alfabetico il Glossario dei termini e degli Acronimi ritenuti di particolare importanza.

Glossario dei Termini	
Accesso	Operazione che consente di prendere visione dei documenti informatici.
Affidabilità	Caratteristica che, con riferimento a un sistema di gestione documentale o conservazione, esprime il livello di fiducia che l'utente ripone nel sistema stesso, mentre con riferimento al documento informatico esprime la credibilità e l'accuratezza della rappresentazione di atti e fatti in esso contenuta.
Aggregazione documentale informatica	Insieme di documenti informatici o insieme 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 dei documenti prodotti o acquisiti da un soggetto pubblico o privato durante lo svolgimento della propria attività.
Archivio informatico	Archivio costituito da documenti informatici, organizzati in aggregazioni documentali informatiche.

Area Organizzativa Omogenea	Un insieme di funzioni e di uffici individuati dall'ente al fine di gestire i documenti in modo unitario e coordinato, secondo quanto disposto dall'art. 50 comma 4 del D.P.R. 28 dicembre 2000, n. 445. Essa rappresenta il canale ufficiale per l'invio di istanze e l'avvio di procedimenti amministrativi.
Attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico	Dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico.

Autenticità	Caratteristica in virtù della quale un oggetto deve considerarsi come corrispondente a ciò che era nel momento originario della sua produzione. Pertanto un oggetto è autentico se nel contempo è integro e completo, non avendo subito nel corso del tempo o dello spazio alcuna modifica non autorizzata. L'autenticità è valutata sulla base di precise evidenze.
Certificazione	Attestazione di terza parte relativa alla conformità ai requisiti specificati di prodotti, processi, persone e sistemi.
Classificazione	Attività di organizzazione di tutti i documenti secondo uno schema costituito da un insieme di voci articolate in modo gerarchico e che individuano, in astratto, le funzioni, competenze, attività e/o materie del soggetto produttore.
Codec	Algoritmo di codifica e decodifica che consente di generare flussi binari, eventualmente imbustarli in un file o in un wrapper (codifica), così come di estrarli da esso (decodifica).
Conservatore	Soggetto pubblico o privato che svolge attività di conservazione dei documenti informatici.
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, garantendo nel tempo le caratteristiche di autenticità, integrità, leggibilità, reperibilità dei documenti

Convenzioni di denominazione del file	Insieme di regole sintattiche che definiscono il nome dei file all'interno di un filesystem o pacchetto.
Coordinatore della Gestione Documentale	Soggetto responsabile della definizione di criteri uniformi di classificazione ed archiviazione nonché di comunicazione interna tra le AOO ai sensi di quanto disposto dall'articolo 50 comma 4 del DPR 445/2000 nei casi di amministrazioni che abbiano istituito più AOO.

Documento amministrativo informatico	Ogni rappresentazione, grafica, fotocinematografica, elettromagnetica o di qualunque altra specie, del contenuto di atti, anche interni, formati dalle pubbliche amministrazioni, o, comunque, da queste ultime utilizzati ai fini dell'attività amministrativa
Documento elettronico	Qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva
Documento informatico	Documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
Duplicato informatico	Vedi art. 1, comma 1, lett) i quinquies del CAD.
Estrazione statica dei dati	Estrazione di informazioni utili da grandi quantità di dati (es. database, datawarehouse ecc...), attraverso metodi automatici o semi-automatici
Evidenza informatica	Sequenza finita di bit che può essere elaborata da una procedura informatica.
Fascicolo informatico	Aggregazione documentale informatica strutturata e univocamente identificata contenente atti, documenti o dati informatici prodotti e funzionali all'esercizio di una attività allo svolgimento di uno specifico procedimento.
File	Insieme di informazioni, dati o comandi logicamente correlati, raccolti sotto un unico nome e registrati, per mezzo di un programma di elaborazione o di scrittura, nella memoria di un computer.
Filesystem	Sistema di gestione dei file, strutturato mediante una o più gerarchie ad albero, che determina le modalità di assegnazione dei nomi, memorizzazione e organizzazione all'interno di uno storage.
Firma elettronica	Vedi articolo 3 del Regolamento eIDAS.

Firma elettronica avanzata	Vedi articoli 3 e 26 del Regolamento eIDAS.
Firma elettronica qualificata	Vedi articolo 3 del Regolamento eIDAS.

Formato contenitore	Formato di file progettato per consentire l'inclusione (“imbustamento” o wrapping), in uno stesso file, di una o più evidenze informatiche soggette a differenti tipi di codifica e al quale possono essere associati specifici metadati.
Formato del documento informatico	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l’estensione del file.
Formato “deprecato”	Formato in passato considerato ufficiale il cui uso è attualmente sconsigliato a favore di una versione più recente.
Funzioni aggiuntive del protocollo informatico	Nel sistema di protocollo informatico, componenti supplementari rispetto a quelle minime, necessarie alla gestione dei flussi documentali, alla conservazione dei documenti nonché alla accessibilità delle informazioni.
Funzioni minime del protocollo informatico	Componenti del sistema di protocollo informatico che rispettano i requisiti di operazioni ed informazioni minime di cui all’articolo 56 del D.P.R. 28 dicembre 2000, n. 445.
Funzione di hash crittografica	Funzione matematica che genera, a partire da una evidenza informatica, una impronta crittografica o digest (vedi) in modo tale che risulti computazionalmente difficile (di fatto impossibile), a partire da questa, ricostruire l’evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti.
Gestione Documentale	Processo finalizzato al controllo efficiente e sistematico della produzione, ricezione, tenuta, uso, selezione e conservazione dei documenti.
hash	Termine inglese usato, impropriamente, come sinonimo d’uso di “impronta crittografica” o “digest” (vedi).
Identificativo univoco	Sequenza di numeri o caratteri alfanumerici associata in modo univoco e persistente ad un'entità all'interno di uno specifico ambito di applicazione.
Impronta crittografica	Sequenza di bit di lunghezza predefinita, risultato dell’applicazione di una funzione di hash crittografica a un’evidenza informatica.

Integrità	Caratteristica di un documento informatico o di un'aggregazione documentale in virtù della quale risulta che essi non hanno subito nel tempo e nello spazio alcuna alterazione non autorizzata. La caratteristica dell'integrità, insieme a quella della completezza, concorre a determinare la caratteristica dell'autenticità.

Interoperabilità	Caratteristica di un sistema informativo, le cui interfacce sono pubbliche e aperte, e capaci di interagire in maniera automatica con altri sistemi informativi per lo scambio di informazioni e l'erogazione di servizi.
Leggibilità	Caratteristica di un documento informatico che garantisce la qualità di poter essere decodificato e interpretato da un'applicazione informatica.
Manuale di conservazione	Documento informatico che descrive il sistema di conservazione e illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture.
Manuale di gestione	Documento informatico che 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.
Metadati	Dati associati a un o documento informatico, a un fascicolo informatico o a un'aggregazione documentale per identificarli, descrivendone il contesto e il contenuto - così da permetterne la gestione del tempo - in conformità a quanto definito nella norma ISO 15489-1:2016 e più nello specifico dalla norma ISO 23081-1:2017.
Oggetto di conservazione	Oggetto digitale versato in un sistema di conservazione.
Oggetto digitale	Oggetto informativo digitale, che può assumere varie forme tra le quali quelle di documento informatico, fascicolo informatico, aggregazione documentale informatica o archivio informatico.
Pacchetto di archiviazione	Pacchetto informativo generato dalla trasformazione di uno o più pacchetti di versamento coerentemente con le modalità riportate nel manuale di conservazione.
Pacchetto di distribuzione	Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta di accesso a oggetti di conservazione.

Pacchetto di file (file package)	Insieme finito di più file che costituiscono, collettivamente oltre che individualmente, un contenuto informativo unitario e auto-consistente.
Pacchetto di versamento	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo il formato descritto nel manuale di conservazione.
Pacchetto informativo	Contenitore logico che racchiude uno o più oggetti di conservazione con i relativi metadati, oppure anche i soli metadati riferiti agli oggetti di conservazione.
Pathname	Concatenazione ordinata del percorso di un file e del suo nome.
Percorso	Informazioni relative alla localizzazione virtuale del file all'interno del filesystem espressa come concatenazione ordinata del nome dei nodi del percorso.
Piano della sicurezza del sistema di conservazione	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi.
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.
Piano di classificazione (Titolario)	Struttura logica che permette di organizzare documenti e oggetti digitali secondo uno schema desunto dalle funzioni e dalle attività dell'amministrazione interessata.
Piano di conservazione	Documento, allegato al manuale di gestione e integrato con il sistema di classificazione, in cui sono definiti i 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 di organizzazione delle aggregazioni documentali	Strumento integrato con il sistema di classificazione a partire dai livelli gerarchici inferiori di quest'ultimo e finalizzato a individuare le tipologie di aggregazioni documentali (tipologie di serie e tipologie di fascicoli) che devono essere prodotte e gestite in rapporto ai procedimenti e attività in cui si declinano le funzioni svolte dall'ente

Piano generale della sicurezza	Documento che pianifica le 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.
Presa in carico	Accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione e, in caso di affidamento del servizio all'esterno, dagli accordi stipulati tra il titolare dell'oggetto di conservazione e il responsabile del servizio di conservazione.
Processo	Insieme di attività correlate o interagenti che trasformano elementi in ingresso in elementi in uscita.
Produttore dei PdV	Persona fisica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con il responsabile della gestione documentale.
Rapporto di versamento	Documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore.
Registro di protocollo	Registro informatico ove sono memorizzate le informazioni prescritte dalla normativa per tutti i documenti ricevuti e spediti da un ente e per tutti i documenti informatici dell'ente stesso.
Registro particolare	Registro informatico individuato da una pubblica amministrazione per la memorizzazione delle informazioni relative a documenti soggetti a registrazione particolare.
Regolamento eIDAS	electronic IDentification Authentication and Signature, Regolamento (UE) № 910/2014 del Parlamento Europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.

Repertorio	Registro su cui vengono annotati con un numero progressivo i fascicoli secondo l'ordine cronologico in cui si costituiscono all'interno delle suddivisioni del piano di classificazione.

Responsabile dei sistemi informativi per la conservazione	Soggetto che coordina i sistemi informativi all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID.
Responsabile del servizio di conservazione	soggetto che coordina il processo di conservazione all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
Responsabile della conservazione	Soggetto che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia.
Responsabile della funzione archivistica di conservazione	soggetto che coordina il processo di conservazione dal punto di vista archivistico all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
Responsabile della gestione documentale	Soggetto responsabile della gestione del sistema documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61 del D.P.R. 28 dicembre 2000, n. 445.
Responsabile della protezione dei dati	Persona con conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, in grado di assolvere i compiti di cui all'articolo 39 del Regolamento (UE) 2016/679.
Responsabile della sicurezza dei sistemi di conservazione	soggetto che assicura il rispetto dei requisiti di sicurezza all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
Responsabile dello sviluppo e della manutenzione del sistema di conservazione	soggetto che assicura lo sviluppo e la manutenzione del sistema all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID

Riferimento temporale	Insieme di dati che rappresenta una data e un'ora con riferimento al Tempo Universale Coordinato (UTC).
Riversamento	Procedura mediante la quale uno o più documenti informatici sono convertiti da un formato di file (ovvero di busta, ovvero di pacchetto di file) ad un altro, lasciandone invariato il contenuto per quanto possibilmente permesso dalle caratteristiche tecniche del formato (ovvero dei formati) dei file e delle codifiche di

	destinazione.
Scarto	Operazione con cui si eliminano definitivamente, secondo quanto previsto dalla normativa vigente, i documenti ritenuti non più rilevanti ai fini giuridico-amministrativo e storico-culturale.
Serie	Raggruppamento di documenti con caratteristiche omogenee (vedi anche aggregazione documentale informatica).
Sigillo elettronico	Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica, per garantire l'origine e l'integrità di questi ultimi.
Sistema di conservazione	Insieme di regole, procedure e tecnologie che assicurano la conservazione dei documenti informatici in attuazione a quanto previsto dall'art. 44, comma 1, del CAD.
Sistema di gestione informatica dei documenti	Insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle organizzazioni per la gestione dei documenti. Nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445
Titolare dell'oggetto di conservazione	Soggetto produttore degli oggetti di conservazione.
Trasferimento	Passaggio di custodia dei documenti da una persona o un ente ad un'altra persona o un altro ente.
TUDA	Testo Unico della Documentazione Amministrativa, Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni e integrazioni.
Ufficio	Riferito ad un'area organizzativa omogenea, un ufficio dell'area stessa che utilizza i servizi messi a disposizione dal sistema di protocollo informatico.

Utente abilitato	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.

Versamento	Passaggio di custodia, di proprietà e/o di responsabilità dei documenti. Nel caso di un organo giudiziario e amministrativo dello Stato operazione con la quale il responsabile della conservazione trasferisce agli Archivi di Stato o all'Archivio Centrale dello Stato della documentazione destinata ad essere ivi conservata ai sensi della normativa vigente in materia di beni culturali.

Glossario degli Acronimi	
AGID	Agenzia per l'Italia digitale
AOO	Aree Organizzative Omogenee
CAD	Codice dell'Amministrazione Digitale - Decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni.
eIDAS	Regolamento (UE) № 910/2014 del Parlamento Europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.
FEA	Vedi firma elettronica avanzata.
FEQ	Vedi firma elettronica qualificata.
GDPR	Regolamento (UE) № 679/2016 del Parlamento Europeo e del Consiglio, del 27 aprile 2016 ("General Data Protection Regulation"), 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.
PdA (AiP)	Pacchetto di Archiviazione.
PdD (DiP)	Pacchetto di Distribuzione.
PdV (SiP)	Pacchetto di Versamento.
SPI	Sistema protocollo Informatico
U.O.	Unità organizzativa
UP	Ufficio di protocollo Generale

1.4. Normativa di riferimento

Alla data odierna l'elenco dei principali riferimenti normativi italiani in materia è costituito da:

- **Legge del 7 agosto 1990, n. 241 e successivi aggiornamenti-** Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;

- **Decreto del Presidente della Repubblica del 28 dicembre 2000, n. 445 e (TUDA)** – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- **Decreto legislativo del 30 giugno 2003, n. 196 -** Codice in materia di protezione dei dati personali;
- **Decreto legislativo del 22 gennaio 2004, n. 42 -** Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n.137;
- **Decreto legislativo del 7 marzo 2005, n. 82 e s.m.i.-** Codice dell'Amministrazione digitale;
- **Decreto del Presidente del Consiglio dei Ministri del 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;
- **Decreto legislativo del 14 marzo 2013, n.33 e s.m.i.** Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni;
- **Decreto del Presidente del Consiglio dei Ministri del 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;
- **Decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013** Regole tecniche per il protocollo informatico: art. 2 comma 1, Oggetto e ambito di applicazione; art. 6, Funzionalità; art. 9, Formato della segnatura di protocollo; art. 18 commi 1 e 5, Modalità di registrazione dei documenti informatici; art. 20, Segnatura di protocollo dei documenti trasmessi; art. 21, Informazioni da includere nella segnatura;
- **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;
- **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 AgID del 18 aprile 2017, n. 2 -** recante le misure minime di sicurezza ICT per le pubbliche amministrazioni;
- **Circolare AgID del 9 aprile 2018, n. 2 –** Criteri per la qualificazione dei Cloud Service Provider per la PA;
- **Circolare AgID del 9 aprile 2018, n. 3 –** Criteri per la qualificazione di servizi SaaS per il Cloud della PA;
- **Decreto del Presidente del Consiglio dei Ministri del 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 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 alla generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate;
- **Linee guida del 9 gennaio 2020** sull'Accessibilità degli strumenti informatici. **Linee Guida AgID del 9 settembre 2020** sulla formazione, gestione e conservazione dei documenti informatici e relativi allegati;
- **Circolare AgID n. 2/2021 del 29 marzo 2021,** recante integrazioni alla circolare AgID n. 2 del 9 aprile 2018 «Criteri per la qualificazione dei Cloud Service Provider per la PA» e alla circolare AgID n. 3 del 9 aprile 2018 «Criteri per la qualificazione di servizi SaaS per il Cloud della PA».

1.5. Standard di riferimento

Di seguito sono riportati i principali standard e specifiche tecniche di riferimento nell'ambito della gestione documentale dei documenti informatici e documenti amministrativi informatici, l'affidabilità e la sicurezza informatica.
Dove non sono indicate una versione e/o una data specifica, si intende fare riferimento alla più recente versione disponibile del documento citato:

- **Per la gestione documentale**

UNI ISO 15489-1 - Informazione e documentazione - Gestione dei documenti di archivio - Principi generali sul record management;
UNI ISO 15489-2 -Informazione e documentazione - Gestione dei documenti di archivio – Linee Guida sul record management;
ISO/TS 23081-1 - Information and documentation - Records management processes – Metadata for records – Part 1 – Principles, Quadro di riferimento per lo sviluppo di un sistema di metadati per la gestione documentale;
ISO/TS 23081-2 - Information and documentation - Records management processes – Metadata for records – Part 2 – Conceptual and implementation issues, Guida pratica per l'implementazione;
ISO 16175-1 - (ICA) Information and documentation -- Principles and functional requirements for records in electronic office environments -- Part 1: Overview and statement of principles;
ISO 16175-2 - (ICA) Information and documentation -- Principles and functional requirements for records in electronic office environments -- Part 2: Guidelines and functional requirements for digital records management systems;
ISO 16175-3 - (ICA) Information and documentation -- Principles and functional requirements for records in electronic office environments -- Part 3: Guidelines and functional requirements for records in business system;
ISO 15836 - Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core;
ISO 9001 – Sistemi di gestione per la qualità – Requisiti;

ISO 30300:2011 Information and documentation - Management systems for records - Fundamentals and vocabulary;
ISO 30301:2011 Information and documentation - Management systems for records – Requirements;
ISO 30302:2015 Information and documentation - Management systems for records -

Guidelines for implementation;
ISO/TR 23081-3 - Information and documentation — Managing metadata for records — Part 3: Self-assessment method;
MoReq 2001 Model requirements for the management of electronic records. **MoReq 2** Specification 2008 Model requirements for the management of electronic records – che individua i requisiti funzionali della gestione documentale;
MoReq2010 Modular requirements for records systems.

- **Per la conservazione digitale**

UNI 11386 - Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
ISO 14721 - OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
ISO 15836 - Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core;
ISO/TR 18492 - Long-term preservation of electronic document-based information;
ISO 20652 - Space data and information transfer systems - Producer-Archive interface -Methodology abstract standard;
ISO 20104 - Space data and information transfer systems — Producer-Archive Interface Specification (PAIS):
ISO/CD TR 26102 - Requirements for long-term preservation of electronic records;
SIARD Software Independent Archiving of Relational Databases 2.0;
Ministère de la culture et de la communication, Service interministériel des Archives de France, Standard d'échange de donnéès pour l'archivage. Transfert – Communication –Élimination – Restitution - Modification, ver. 2.1, 2018;
METS - Metadata Encoding and Transmission Standard;
PREMIS – PREservation Metadata: Implementation Strategies;
EAD (3)/ISAD (G);
EAC (CPF)/ISAAR (CPF)/NIERA (CPF);
SCONS2/EAG/ISDIAH;

- **Per affidabilità (certificazione/valutazione autovalutazione)**

ISO 16363 - Space data and information transfer systems -- Audit and certification of trustworthy digital repositories;
ISO 16919 - Space data and information transfer systems -- Requirements for bodies providing audit and certification of candidate trustworthy digital repositories;
ISO 17068 - Information and documentation -- Trusted third party repository for digital records;

- **Per Sicurezza informatica**

ISO/IEC 27001 - Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
ISO/IEC 27017 - Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services;
ISO/IEC 27018 - Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII

processors;
ETSI TS 101 533-1 V1.2.1 - Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
ETSI TR 101 533-2 V1.2.1 - Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni.

2. Aspetti Organizzativi

2.1. Aree Organizzative Omogenee

Il Testo Unico delle disposizioni in materia di documentazione amministrativa (D.P.R. n.445/2000 e s.m.i.) prescrive, all'art. 50 comma 4 che ciascuna pubblica amministrazione individui, nell'ambito del proprio ordinamento, gli uffici da considerare ai fini della gestione unica e coordinata dei documenti per grandi AOO, assicurando criteri uniformi di classificazione e archiviazione.
In tale contesto l'Arnas ha individuato cinque AOO per la gestione coordinata dei documenti, utilizzando un unico sistema di protocollazione codificato con un unico titolario di classificazione e producendo un unico archivio.

2.2. Accreditamento delle AOO all'IPA

Per la gestione dei documenti, l'Arnas, ai sensi della normativa vigente, individua le seguenti Aree Organizzative Omogenee (AOO):

- Direzione Aziendale il cui Codice univoco AOO è A49109B;
- Servizio Risorse Umane il cui Codice univoco AOO è A39A9B1;
- Provveditorato Economato il cui Codice univoco AOO è A9CD524;
- Affari Generali il cui Codice univoco AOO è A3355F4;
- Servizio Tecnico il cui Codice univoco AOO è A402796.

L'Azienda, nell'ambito degli adempimenti previsti, è accreditata presso l'Indice delle Pubbliche Amministrazioni (IPA), tenuto e reso pubblico dal DigitPA, raggiungibile da qualsiasi utente all'indirizzo http://www.digitpa.gov.it/.

Il codice identificativo dell'AOO presso l'Indice delle Pubbliche Amministrazioni (Codice IPA) è "aocdcb".

L'Arnas ha effettuato l'iscrizione delle caselle di posta elettronica certificata istituzionale di ogni AOO presso l'IPA:

- ARNAS Ospedali Civico Di Cristina: ospedalecivicopa@pec.it;
- Servizio Affari Generali: sfm.ospedalecivicopa@pec.it;
- Servizio Economico Finanziario: sef.ospedalecivicopa@pec.it;
- Servizio Risorse umane: aru.ospedalecivicopa@pec.it;
- Servizio Provveditorato Economato: ape.ospedalecivicopa@pec.it;
- Servizio Tecnico: tec.ospedalecivicopa@pec.it.

2.3. Ruoli e responsabilità

Per le AOO dell'Arnas sono individuati i seguenti ruoli con responsabilità:

Arnas per tutte le AOO	**Riferimento**	**Email/Pec**
Resp. della Conservazione	**Ing. Stefania Calafiore**	stefania.calafiore@arnascivico.it
Resp. dei Sistemi Informativi	**Dott. Vincenzo Cardinale**	vincenzo.cardinale@arnascivico.it
Resp. della Gestione Documentale	**Arch. Alba Cristodaro**	alba.cristodaro@arnascivico.it
Referente Ufficio Protocollo Generale e Archivio	**Dott.ssa Teresa Gagliano**	teresa.gagliano@arnascivico.it
Resp. della Transizione Digitale	**Dott. Vincenzo Cardinale**	vincenzo.cardinale@arnascivico.it

Di seguito sono elencati i compiti del **Responsabile della gestione documentale**:

- attribuisce il livello di autorizzazione per l'accesso alle funzioni della procedura di protocollazione, distinguendo tra abilitazioni alla consultazione e abilitazioni all'inserimento;
- garantisce che le operazioni di registrazione e di segnatura di protocollo si svolgano nel rispetto delle disposizioni del testo unico delle amministrazioni;
- garantisce la corretta produzione e la conservazione del registro giornaliero di protocollo;
- cura che le funzionalità del sistema in caso di guasti o anomalie siano ripristinate entro ventiquattro ore dal blocco delle attività e, comunque, nel più breve tempo possibile;
- assicura la trasmissione del pacchetto di versamento al sistema di conservazione, secondo le modalità operative definite nel manuale di conservazione;
- provvede a verificare il buon esito della operazione di trasferimento al sistema di conservazione tramite la presa visione del rapporto di versamento prodotto dal sistema di conservazione stesso;
- garantisce il buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, incluse le funzionalità di accesso e le attività di gestione degli archivi;
- vigila sull'osservanza delle disposizioni del testo unico delle amministrazioni (TUDA) da parte del personale autorizzato e degli incaricati;
- predispone il manuale di gestione documentale 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;
- verifica periodicamente la rispondenza del piano di classificazione dei documenti

informatici ai procedimenti amministrativi e agli affari in essere e procede al suo aggiornamento;
- assicura l'adozione di criteri uniformi per la gestione informatica dei documenti;
- verifica l'avvenuta eliminazione dei protocolli di settore, dei protocolli multipli e, più in generale, dei protocolli diversi dal protocollo informatico previsto dal TUDA.

Di seguito sono elencati i compiti del **Responsabile della transizione digitale:**
- coordina lo sviluppo dei sistemi informativi, di telecomunicazione e fonia, in modo da assicurare anche la coerenza con gli standard tecnici e organizzativi comuni;
- indirizza e coordina lo sviluppo dei servizi, sia interni che esterni, forniti dai sistemi informativi di telecomunicazione e fonia dell'amministrazione;
- indirizza, pianifica, coordina e monitora la sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture anche in relazione al sistema pubblico di connettività;
- garantisce l'accesso dei soggetti disabili agli strumenti informatici e promuove l'accessibilità anche in attuazione di quanto previsto dalla legge 9 gennaio 2004, n. 4;
- analizza periodicamente la coerenza tra l'organizzazione dell'amministrazione e l'utilizzo delle tecnologie dell'informazione e della comunicazione, al fine di migliorare la soddisfazione dell'utenza e la qualità dei servizi nonché di ridurre i tempi e i costi dell'azione amministrativa;
- coopera alla revisione della riorganizzazione dell'amministrazione ai fini del punto precedente;
- indirizza, coordina e monitora la pianificazione prevista per lo sviluppo e la gestione dei sistemi informativi di telecomunicazione e fonia;
- progetta e coordina le iniziative rilevanti ai fini di una più efficace erogazione di servizi in rete a cittadini e imprese mediante gli strumenti della cooperazione applicativa tra pubbliche amministrazioni, ivi inclusa la predisposizione e l'attuazione di accordi di servizio tra amministrazioni per la realizzazione e compartecipazione dei sistemi informativi cooperativi;
- promuove le iniziative attinenti all'attuazione delle direttive impartite dal Presidente del Consiglio dei Ministri o dal Ministro delegato per l'innovazione e le tecnologie;
- pianifica e coordina il processo di diffusione, all'interno dell'amministrazione, dei sistemi di identità e domicilio digitale, posta elettronica, protocollo informatico, firma digitale o firma elettronica qualificata e mandato informatico, e delle norme in materia di accessibilità e fruibilità nonché del processo di integrazione e interoperabilità tra i sistemi e servizi dell'amministrazione;
- pianifica e coordina gli acquisti di soluzioni e sistemi informatici, telematici e di telecomunicazione al fine di garantire la compatibilità con gli obiettivi di attuazione dell'agenda digitale e, in particolare, con quelli stabiliti nel piano triennale di cui all'articolo 16, comma 1, lettera b) del CAD.

I compiti del **Responsabile della Conservazione** sono descritti nel Manuale di Conservazione.

Di seguito sono elencati i compiti del **Responsabile dei sistemi informativi:**
- opera d'intesa con il responsabile della conservazione e può affidare, ai sensi dell'articolo 34, comma 1-bis, lettera b) del CAD, la conservazione dei documenti informatici ad altri soggetti, pubblici o privati, che offrono idonee garanzie

organizzative, e tecnologiche e di protezione dei dati personali;
- gestisce l'esercizio delle componenti hardware e software;
- monitora il mantenimento dei livelli di servizio (SLA) concordati con il fornitore e segnala eventuali difformità degli SLA e individuazione e pianificazione delle necessarie azioni correttive;
- pianifica lo sviluppo delle infrastrutture tecnologiche;
- controlla e verifica i livelli di servizio erogati da terzi con segnalazione delle eventuali difformità.

2.4. Attività delle AOO e Ufficio Protocollo Generale

Ciascuna AOO cura la protocollazione dei documenti in Entrata e in uscita utilizzando un'unica sequenza numerica, nel senso che tutta la corrispondenza è gestita attraverso un unico applicativo informatico per la gestione del protocollo.
Il Sistema del protocollo informatico (SPI), la gestione dei flussi documentali e degli archivi dedicati è assicurato dall'Ufficio Protocollo Generale e Archivio (UP) che fa capo alla U.O.C. "Affari Generali".

Gli operatori dell'Ufficio Protocollo sono abilitati alle seguenti operazioni:

- immissione protocollo in entrata e in uscita;
- assegnazione della posta ai vari Uffici/Servizi;
- ricerca dati;
- visione e stampa dei documenti protocollati e archiviati.

3. Formazione dei documenti

Secondo quanto previsto dall'art. 40, comma 1 del CAD, le pubbliche amministrazioni formano gli originali dei propri documenti con mezzi informatici.

3.1. Documento Amministrativo

Ai sensi dell'articolo 22, comma 1, lettera d), della legge n. 241/1990, per documento amministrativo si intende "ogni rappresentazione grafica, foto, cinematografica, elettromagnetica, informatica o di qualunque altra specie del contenuto di atti, anche interni o non relativi ad uno specifico procedimento, detenuti da una pubblica amministrazione e contenenti attività di pubblico interesse, indipendentemente dalla natura pubblicistica o privatistica della loro disciplina sostanziale".

3.1.1 Classificazione in termini tecnologici

3.1.1.1 Documento informatico

Il documento amministrativo informatico è la rappresentazione, mediante dati binari associati a un formato, del contenuto di atti, fatti, o dati giuridicamente rilevanti espressi mediante un testo, un'immagine, un filmato, una riproduzione sonora. Il documento informatico è memorizzato su un supporto fisico che può essere di vari tipi ed è leggibile solo mediante l'ausilio di strumenti tecnologici.

3.1.1.2 Documento Analogico

Il documento amministrativo analogico è la rappresentazione, mediante dati continui memorizzati su un supporto analogico, del contenuto di atti, fatti o dati giuridicamente rilevanti espressi mediante un testo, un'immagine, un filmato, una riproduzione sonora.

3.1.2 Classificazione in termini operativi

3.1.2.1 Documento ricevuto

Sono documenti con rilevanza giuridico probatoria, provenienti da un diverso soggetto pubblico o privato e acquisiti dalla AOO. I documenti possono essere acquisiti con diversi mezzi e modalità in base alla tecnologia utilizzata dal mittente.
Il documento informatico può essere recapitato:

- a mezzo posta elettronica convenzionale o certificata;
- a mezzo posta ordinaria e raccomandata;
- con consegna diretta da parte dell'interessato agli uffici aperti al pubblico.

3.1.2.2 Documento inviato

Sono documenti, con rilevanza informativa e/o giuridico probatoria, provenienti dagli Uffici delle AOO e indirizzati a un diverso soggetto pubblico o privato.
Il documento può essere inviato:

- a mezzo posta elettronica convenzionale o certificata;
- a mezzo posta ordinaria e raccomandata;
- su supporto rimovibile;
- a mezzo corriere interno.

I documenti informatici, compresi di eventuali allegati, sono inviati, di norma, per mezzo della sola posta elettronica certificata se la dimensione del documento e/o di eventuali allegati, non supera la dimensione prevista dal sistema di posta utilizzato dalle AOO.
In caso contrario, il documento informatico viene trasmesso al destinatario con altri mezzi verificandone l'autenticità e l'integrità.

3.1.2.3 Documento interno formale

I documenti interni formali sono documenti di rilevanza amministrativa giuridico-probatoria, redatti al fine di documentare fatti, stati o qualità inerenti alle attività svolte e alle azioni amministrative intraprese, ovvero qualsiasi documento dal quale possano nascere diritti, doveri o legittime aspettative di terzi. Sono formati, di norma, con tecnologie informatiche e sono soggetti a protocollazione.

3.1.2.4 Documento interno informale

I documenti interni informali sono documenti di rilevanza esclusivamente interna a ciascuna Struttura dell'Arnas e, di norma, scambiati attraverso lo strumento della posta elettronica. Le modalità di formazione e gestione sono demandate, nei limiti della propria autonomia organizzativa, a ciascuna Struttura. Per tali documenti non vige l'obbligatorietà di sottoscrizione e protocollazione.

3.2 Requisiti Informatici di scambio con l'esterno

Gli strumenti informatici di scambio garantiscono gli standard di composizione dei messaggi in termini di interoperabilità e di requisiti minimi di sicurezza come di seguito richiamati:

- integrità del messaggio;
- riservatezza del messaggio;
- non ripudio del messaggio;
- automazione dei processi di protocollazione e smistamento dei messaggi all'interno delle AOO;
- certificazione dell'avvenuto inoltro e ricezione;
- interoperabilità dei sistemi informativi pubblici.

3.3 Protocollo informatico

Ai sensi dell'art. 56 TUDA, "le operazioni di registrazione indicate all'articolo 53 e le operazioni di segnatura di protocollo di cui all'articolo 55 nonché le operazioni di classificazione costituiscono operazioni necessarie e sufficienti per la tenuta del sistema di gestione informatica dei documenti da parte delle pubbliche amministrazioni".

Pertanto, il "Protocollo" è la componente minima del sistema di "Sistema di Gestione Informatica dei Documenti" che assicura la gestione contemporanea della registrazione di protocollo e segnatura di protocollo, ovvero:

- registrazione di protocollo: attività di memorizzazione dei dati necessari a conservare le informazioni per ogni documento ricevuto o spedito o interno;
- segnatura di protocollo: apposizione o associazione all'originale del documento, in forma permanente non modificabile, dei metadati riguardanti il documento stesso funzionali alla ricezione o spedizione.

Il sistema di gestione del protocollo è esclusivamente di tipo informatico. Non sono ammessi registri di protocollo cartacei.
Il relativo software garantisce l'immodificabilità delle registrazioni di protocollo nonché la contemporaneità della stessa con l'operazione di segnatura.
La descrizione funzionale ed operativa del sistema informatico è contenuta nel manuale del sistema di protocollo informatico, disponibile sul software stesso.

3.4 Firma digitale

La firma digitale utilizzata per inviare e ricevere documenti da e per l'Azienda e per sottoscrivere documenti o qualsiasi altro file digitale con valenza giuridico-probatoria, costituisce l'unico strumento che soddisfa i requisiti di sicurezza, identificabilità del sottoscrittore, nonché integrità ed immodificabilità del documento.
Il documento informatico dotato di firma digitale - avente un certificato valido - va considerato equivalente al documento cartaceo dotato di firma autografa e fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni di chi lo ha sottoscritto; il documento dotato di firma elettronica, o "firma digitale debole", sul piano probatorio, invece, è liberamente valutabile in giudizio.
Nel Sistema di protocollo informatico (Spi) sono previste funzioni automatiche di verifica della firma digitale apposta dall'utente sui documenti e sugli eventuali allegati da fascicolare.
L'Azienda ha avviato un processo di informatizzazione fornendo la firma elettronica per

tutti i dipendenti che per funzione e competenza sottoscrivono atti di rilevanza giuridica.

3.5 Posta Elettronica e PEC

In conformità all'art. 47, comma 3 del CAD, le comunicazioni tra l'Arnas e i propri dipendenti, così come tra le diverse strutture aziendali, avvengono prevalentemente attraverso l'utilizzo delle caselle di posta elettronica istituzionali, nel pieno rispetto della normativa sulla protezione dei dati personali.

Per le comunicazioni con altre Pubbliche Amministrazioni, aziende, ditte e persone giuridiche, l'Arnas utilizza la posta elettronica certificata (PEC), in linea con le disposizioni normative vigenti. La PEC è impiegata per:

- l'invio di documenti amministrativi, previa registrazione al protocollo;
- comunicazioni che richiedono una ricevuta di invio e/o di consegna;
- documenti il cui contenuto impegna formalmente l'Arnas nei confronti di terzi.

4. Regole di assegnazione

L'attività di assegnazione consiste nell'individuare la U.O. che avrà la responsabilità della gestione del documento protocollato. Tale attività è svolta direttamente dall'Ufficio Protocollo tramite apposito applicativo.
Il processo di assegnazione è effettuato sulla base dell'organigramma e del funzionigramma aziendale, all'assegnazione per competenza consegue la responsabilità del procedimento amministrativo.
L'assegnazione può essere effettuata, oltre che per competenza, anche per conoscenza.
L'U.O. competente è incaricata della gestione del procedimento a cui il documento si riferisce e prende in carico il documento. I termini per la definizione del procedimento amministrativo che prende avvio dal documento decorrono comunque dalla data di protocollazione.
I documenti sono di norma assegnati il giorno di ricezione o comunque entro il giorno successivo, salvo che figurino, entro detto lasso di tempo, uno o più giorni non lavorativi, nel qual caso l'operazione di protocollazione viene assicurata entro le 24 ore dall'inizio del primo giorno lavorativo successivo.

4.1. Documenti ricevuti in formato digitale

I documenti ricevuti dalle AOO per via telematica, o comunque disponibili in formato digitale, sono assegnati all'U.O. competente attraverso i canali telematici al termine delle operazioni di registrazione, segnatura di protocollo, memorizzazione su supporti informatici in modo non modificabile.

L'acquisizione dei documenti informatici viene registrata dal SPI in modo automatico e la data di ingresso dei documenti nelle UU.OO. competenti coincide con la data di assegnazione degli stessi.
Le UU.OO. sono altresì in grado di visualizzare i documenti assegnati per conoscenza e, in base alle abilitazioni possedute, potranno:

- visualizzare gli estremi del documento;
- visualizzare il contenuto del documento;

- verificare l'U.O. a cui il documento è assegnato per competenza.

4.2. Documenti ricevuti in formato cartaceo

I documenti ricevuti dall'AOO in formato cartaceo, al termine delle operazioni di registrazione e segnatura informatica, sono assegnati all'ufficio di competenza per via informatica attraverso la rete interna dell'amministrazione.

4.3. Assegnazione di documenti in uscita o a rilevanza interna

Per la corrispondenza in uscita, l'ufficio che ha prodotto il documento e che lo protocolla provvede ad assegnarlo a sé stesso per competenza.
Qualora la formazione e la protocollazione del documento sia stata effettuata per conto di altro ufficio, che sia competente per materia, l'assegnazione per competenza deve essere effettuata a quest'ultimo, lasciando la conoscenza all'Ufficio che ha proceduto alle operazioni di protocollazione e spedizione.

4.4. Modifica delle assegnazioni

Nel caso di assegnazione per competenza errata, l'U.O. che riceve il documento comunica al più presto l'errore all'Ufficio Protocollo, specificando – ove possibile – l'esatta competenza.
L'Ufficio Protocollo provvede alla riassegnazione, correggendo le informazioni inserite nel sistema informatico e inviando il documento all'U.O. competente.
Qualora vi siano difficoltà di individuazione dell'ufficio competente per l'assegnazione, ovvero restituzione del medesimo documento da parte di più uffici, la decisione sull'assegnazione è demandata al Direttore Amministrativo. Il sistema di gestione informatica del protocollo tiene traccia di tutti i passaggi memorizzando l'identificativo dell'utente che effettua l'operazione con la data e l'ora di esecuzione.
Non è prevista la restituzione di documentazione assegnata per conoscenza.

4.5. Classificazione

Tutti i documenti ricevuti o prodotti, indipendentemente dal supporto sul quale sono formati, sono classificati in base al Titolario di classificazione. La classificazione di primo livello dei documenti in arrivo è inserita dall'Ufficio Protocollo, mentre l'U.O. assegnataria completa l'informazione con il secondo livello di classificazione.

5. Abilitazioni al sistema di gestione informatica dei documenti

5.1. Criteri generali

I nuovi utenti vengono abilitati all'accesso al sistema informatico di protocollo e gestione documentale Archiflow, dall'UO ICT Management su richiesta formulata dal Responsabile del Servizio presso cui operano. L'accesso al sistema è consentito unicamente al personale dell'Arnas, non vengono pertanto rilasciate abilitazioni a soggetti esterni all'Amministrazione. Ogni utente abilitato accede al sistema utilizzando le proprie credenziali di dominio (User e password).

5.2. Abilitazione alle funzioni di visualizzazione

Il sistema informatico garantisce la riservatezza delle informazioni, consentendo di limitare la visibilità dei documenti/registrazioni ai soli utenti che possiedono uno specifico livello di abilitazione. In particolare, gli utenti sono abilitati alla visione dei soli documenti/registrazioni da essi stessi caricati nel sistema, o di quelli assegnati per competenza o conoscenza.

5.3. Gestione dei log di sistema

Il sistema Archiflow è predisposto per tracciare eventi o azioni compiute dagli utenti e dagli amministratori durante l'uso del protocollo informatico e la gestione documentale (c.d. "Log").

6. Formati dei documenti informatici previsti dalle LLGG

I documenti informatici prodotti dall'Arnas, quali rappresentazioni informatiche di atti, fatti o dati giuridicamente rilevanti, indipendentemente dal software utilizzato, sono convertiti in uno dei formati standard previsti dalla normativa vigente in materia di conservazione, al fine di garantire la loro inalterabilità durante le fasi di accesso e conservazione, nonché l'immutabilità nel tempo del contenuto.
La Tabella successiva riassume i formati dei documenti utilizzati per ciascuna classe documentale.

Classe Documentale	Descrizione	Formato
Fatture PA Attive	Fatture Attive verso la PA	XML, P7M
Fatture PA Passive	Fatture Passive da PA e fornitori	XML, P7M
Notifiche SDI Fatture PA Attive	Notifiche SDI relative a Fatture Attive verso la PA	XML, P7M
Notifiche SDI Fatture PA Passive	Notifiche SDI relative a Fatture Passive da PA e fornitori	XML, P7M
Delibere	Atti di direzione - Delibere	PDF, P7M
Determine	Atti di direzione - Determine	PDF, P7M
Documenti Protocollati	Documenti oggetto di protocollo	pdf, p7m, eml, jpeg, txt, tiff, docx, xlsx, xml, odb, odc, odf, odg, odp, msbmp, odt, ods, zip, mspp, rar, 7z, dwfz, png, html, dwf, sxw, dwg, psd, lwp, gif, tsr, dxf,

		data, vcf, rtf, wmz, json, p7s, ppt, pptx, msa, xls, mp3
Repertori – Registro Giornaliero di Protocollo	Registri di protocollo, deliberazione, contratti, convenzioni, ecc. (documenti amministrativi elettronici)	PDF
Ricette Dematerializzate Erogate	Ricette elettroniche dematerializzate erogate	ZIP, XML
Ricette Dematerializzate Erogate Annullate	Ricette elettroniche dematerializzate erogate e annullate	ZIP, XML
Ricette Dematerializzate Prescritte	Ricette elettroniche dematerializzate prescritte	ZIP, XML
Ricette Dematerializzate Prescritte Annullate	Ricette elettroniche dematerializzate prescritte e annullate	ZIP, XML
Immagini in ambito di diagnostica sanitaria	Immagini in ambito di diagnostica sanitaria	DICOM

7. Protocollo informatico e registrazioni particolari

La descrizione funzionale ed operativa del sistema informatico è contenuta nel manuale del sistema di protocollo informatico Archiflow.

7.1. Registro di emergenza

Qualora non sia possibile fruire del SPI per una interruzione accidentale o programmata, per oltre le 48 ore, su disposizione del Direttore Generale, potrà essere attivata la procedura di emergenza, mediante la registrazione della corrispondenza su un documento cartaceo, denominato "Registro di emergenza" (art. 63 DPR 445/2000) Allegato 1.

Il “registro di emergenza” (Allegato mod. 3) è individuato univocamente da tre elementi: codice UO, numero documento, data documento.

Il “registro di emergenza” può essere attivato contemporaneamente anche da più AOO, e la numerazione parte da 1 per ogni giorno solare.

Il Direttore Generale è colui che autorizza e revocherà l’utilizzo del registro di emergenza compilando i seguenti modelli:

- AUTORIZZAZIONE ALLO SVOLGIMENTO DELLE OPERAZIONI DI

REGISTRAZIONE DI PROTOCOLLO SUL REGISTRO DI EMERGENZA (art. 63 DPR 445/2000). Allegato mod. n° 1;

- REVOCA AUTORIZZAZIONE ALLO SVOLGIMENTO DELLE OPERAZIONI DI REGISTRAZIONE DI PROTOCOLLO SUL REGISTRO DI EMERGENZA(art. 63 DPR 445/2000). Allegato mod. n° 2.

Una volta revocate le operazioni in emergenza, i documenti registrati dovranno essere protocollati sul SPI con la normale procedura ai quali viene attribuito un nuovo numero di protocollo generale, continuando la numerazione raggiunta al momento dell'interruzione del servizio. A tale registrazione sono associati anche il numero di protocollo e la data di registrazione riportati sul protocollo di emergenza. I documenti annotati nel registro di emergenza e trasferiti nel protocollo generale recano, pertanto, due numeri, quello del protocollo di emergenza e quello del protocollo generale.

Al termine delle suddette operazioni, tutti i registri protocollo insieme all'autorizzazione e alla revoca, andranno protocollati.

La data in cui è stata effettuata la protocollazione sul registro di emergenza è quella a cui si fa riferimento per la decorrenza dei termini del procedimento amministrativo. In tal modo è assicurata la corretta sequenza dei documenti che fanno parte di un determinato procedimento amministrativo.

7.2. Elenco dei documenti esclusi dalla registrazione di protocollo

Non sono soggette a protocollazione le seguenti tipologie documentali:

- le tipologie espressamente previste dall'art. 53, comma 5 del DPR 445/2000 (bollettini ufficiali PA, notiziari PA, materiali statistici, giornali, riviste);
- i documenti soggetti a registrazione particolare (delibere, determine, disposizioni, decreti, ordini di fornitura, fatture emesse e ricevute);
- i documenti che costituiscono mera notizia di prevalente rilevanza informativa ;
- i documenti clinici.

8. Titolario di classificazione

Il Titolario di classificazione è allegato al presente documento.

9. Fascicolazione

La fascicolazione è l'attività di riconduzione logica (e, nel caso di documenti cartacei, anche fisica) di un documento all'interno dell'unità archivistica che ne raccoglie i precedenti, al fine di mantenere vivo il vincolo archivistico che lega ogni singolo documento alla pratica relativa. Tale attività permette di costruire un sistema basato sull'organizzazione funzionale dei documenti in unità complesse stabili nel tempo (i fascicoli), che riflettono la concreta attività del soggetto produttore. La classificazione e la fascicolazione favoriscono la sedimentazione stabile dei documenti prodotti e acquisiti dall'Amministrazione nel corso della propria attività: solo così si assicura la possibilità per l'Amministrazione stessa e per il cittadino di accedere ad una informazione contestualizzata, che dia conto del patrimonio informativo utilizzato a supporto di una determinata attività amministrativa (definizione AgiD).

La procedura di fascicolazione è prevista nell'applicativo di protocollazione Archiflow ed è in corso di implementazione da parte dell'Arnas.

10. Flussi di lavorazione dei documenti protocollati

10.1. Flusso dei documenti ricevuti dalle AOO

Il sistema di protocollo informatico (Archiflow) accede direttamente alle caselle PEC istituzionali delle AOO dell' ARNAS e scarica i messaggi ad essa pervenuti.

Il sistema consente di ricevere documenti pervenuti via PEC da un'altra Pubblica Amministrazione acquisendo i dati necessari alla protocollazione direttamente dalla segnatura XML allegata ai documenti stessi.

La ricezione di documenti comporta l'invio al mittente di due diverse ricevute, entrambe legate al servizio di posta certificata: la prima è relativa all'accettazione della Pec, la seconda all'effettiva consegna del messaggio.

La posta elettronica ordinaria (PEO), al contrario della email PEC, non permette di identificare con certezza il mittente di una comunicazione, né ha data certa.
La PEO, tuttavia, rappresenta un mezzo riconosciuto di trasmissione di documenti: l'art. 65 del CAD consente infatti al cittadino di presentare istanze e dichiarazioni per via telematica alle pubbliche amministrazioni qualora esse siano sottoscritte e presentate unitamente alla copia del documento d'identità. I documenti ricevuti via posta elettronica ordinaria dalle U.O. dell'Arnas e ai quali sia necessario attribuire efficacia probatoria, vanno inoltrati alla AOO di riferimento che provvederà alla loro registrazione nel SPI.

Il Servizio Protocollo apre tutte le buste pervenute, compresa la corrispondenza nominativamente intestata qualora essa sia riferibile ad attività istituzionale, ed è registrata e sottoscritta tramite segnatura ad eccezione della corrispondenza esclusa dalla protocollazione (ved. punto 7.2).

In considerazione dell'art. 616 C.P. fanno eccezione, e pertanto non vengono aperte, le buste con le caratteristiche seguenti:

- riportanti le seguenti diciture: "riservato", "personale", "confidenziale" o comunque dalla cui confezione si evinca il carattere di corrispondenza privata; a titolo di esempio si riportano qui di seguito alcune delle casistiche più frequenti, con l'indicazione del comportamento da seguire:
  - Mario Rossi c/o Ufficio XY (NON APRIRE);
  - Mario Rossi (NON APRIRE);
  - Arnas c.a. Mario Rossi (APRIRE);
  - Arnas Mario Rossi (APRIRE);
- la corrispondenza personale viene consegnata al destinatario, il quale, dopo averne preso visione, se reputa che i documenti ricevuti debbano essere comunque protocollati perché riguardanti problematiche istituzionali, provvede a trasmetterli al UP per la protocollazione. In caso di corrispondenza personale ricevuta tramite raccomandata o corriere, al momento del ritiro il destinatario firma apposita ricevuta di avvenuta consegna;
- riportanti le seguenti diciture: "offerta", "bando", "gara d'appalto" o simili, o comunque dalla cui confezione si evinca la partecipazione ad una gara (ad esempio: presenza di sigilli in ceralacca, firme apposte sui lembi della busta, ecc.);

- indirizzate ad Enti diversi dalla Arnas;
- indirizzate a una delle Associazioni operanti all'interno dell'Arnas.

Gli addetti all'Ufficio Protocollo non possono rilasciare ricevute per i documenti che non sono soggetti a protocollazione.
La semplice apposizione del timbro datario sulla copia, non ha alcun valore giuridico e non comporta alcuna responsabilità del personale dell'Ufficio Protocollo in merito alla ricezione ed all'assegnazione del documento.

Quando il documento cartaceo è consegnato direttamente dal mittente, o da altra persona incaricata all'Ufficio Protocollo Generale, ed è richiesto il rilascio di una ricevuta attestante l'avvenuta consegna, l'operatore che lo riceve è autorizzato a:

- fotocopiare gratuitamente la prima pagina del documento;
- apporre gli estremi della segnatura se contestualmente alla ricezione avviene anche la protocollazione;
- apporre sulla copia così realizzata il timbro di ricevuta con la data e l'ora d'arrivo e la propria sigla.

Per la corrispondenza consegnata da corrieri, viene timbrata la bolletta di consegna con timbro datario e firma dell'addetto ricevente.

Le buste pervenute tramite posta, corriere o altra modalità per la quale si renda rilevante evidenziare il mezzo di trasmissione, sono spillate insieme al documento e trasmesse alla U.O. di competenza.

10.2. Flusso dei documenti inviati dall'Arnas

La trasmissione dei documenti informatici soggetti alla registrazione di protocollo può essere effettuata dall'Arnas mediante messaggi di posta elettronica certificata.
Per la protocollazione dei messaggi PEC in uscita, si procede secondo la modalità di seguito descritta:

- firma del documento (firma digitale del documento informatico, preventivamente trasformato in formato pdf, o firmato in modo autografo e scansionato in pdf);
- registrazione sull'applicativo Archiflow, con specifica del mezzo di spedizione e indicazione dell'indirizzo PEC del destinatario, inserimento della scansione, protocollazione e contestuale invio (esclusivamente dalla PEC istituzionale).

Per ogni documento cartaceo destinato ad essere spedito in originale vengono prodotti, di norma, tanti esemplari quanti sono i destinatari.

L'originale rappresenta la redazione definitiva, perfetta e autentica negli elementi sostanziali e formali.
Le copie trasmesse per ragioni amministrative ad altre strutture organizzative sono conservate per tutto il tempo necessario allo svolgimento del procedimento cui il documento si riferisce e quindi eliminate secondo le norme previste.
Nello specifico per quanto riguarda il regime giuridico delle copie informatiche di documento analogico/cartaceo si rimanda agli articoli 23-ter c. 3 del CAD (copie informatiche di documenti formati in origine su supporto analogico, da intendersi quale "documento informatico avente contenuto identico a quello del documento da cui è tratto") e all'art. 22 c. 2 del CAD (copie per immagine su supporto informatico di

documento analogico, da intendersi quale “documento informatico avente contenuto e forma identici a quelli del documento analogico da cui è tratto”).

L’ufficio Protocollo Generale espleta direttamente tutte le operazioni di spedizione della corrispondenza provvedendo:

- all’affrancatura;
- alla predisposizione della distinta delle raccomandate, da consegnare all'ufficio postale;
- alla consegna all'ufficio postale attraverso il servizio Autisti;

Le cartoline di ritorno delle raccomandate sono compilate dall’U.O. mittente, che avrà cura di indicare su di esse la denominazione del proprio Ufficio, al fine di consentire il corretto smistamento delle cartoline al momento della loro successiva ricezione dal Protocollo Generale.

10.3. Formazione dei documenti - Aspetti operativi

Il contenuto minimo dei documenti informatici deve garantire la presenza delle seguenti informazioni:

- **denominazione dell’amministrazione,** comprensiva del codice fiscale o partita IVA e del codice identificativo dell’amministrazione; per quanto riguarda i documenti su supporto cartaceo si utilizza il formato predisposto dall’amministrazione (carta intestata);
- **indicazione del settore, servizio o ufficio** che ha prodotto il documento;
- **indirizzo completo** (via, numero civico, codice avviamento postale, città, sigla della provincia, numero di telefono, indirizzo di posta elettronica dell’ente, PEC);
- **data**: luogo, giorno, mese, anno;
- **destinatario**, per i documenti in partenza;
- **oggetto del documento**, sufficientemente esaustivo del testo (ogni documento deve trattare un solo oggetto);
- **classificazione** (categoria, classe e fascicolo);
- **numero degli allegati**, se presenti;
- **numero di protocollo**;
- **testo**;
- **indicazione dell’autore del documento** (nome e cognome anche abbreviato);
- **estremi identificativi del Responsabile del procedimento** (l. 241/1990);
- **sottoscrizione autografa o elettronico/digitale.**

10.4. Unicità del protocollo informatico

Nell’ambito dell’Arnas il registro generale di protocollo è unico al pari della numerazione progressiva delle registrazioni di protocollo.
La numerazione si chiude al 31 dicembre di ogni anno e ricomincia dal primo gennaio dell’anno successivo.
Il numero di protocollo individua un unico documento e, di conseguenza, ogni documento reca un solo numero di protocollo.
Non è consentita l’identificazione dei documenti mediante l’assegnazione manuale di numeri di protocollo che il sistema informatico ha già attribuito ad altri documenti, anche se questi documenti sono strettamente correlati tra loro. Non è inoltre consentita in nessun caso la cosiddetta registrazione “a fronte”, cioè l’utilizzo di un unico numero di protocollo per il documento in arrivo e per il documento in partenza.

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.
Il registro di protocollo è soggetto alle forme di pubblicità e di tutela di situazioni giuridicamente rilevanti previste dalla normativa vigente. Sono oggetto di registrazione obbligatoria i documenti ricevuti e spediti dall'amministrazione e tutti i documenti informatici, fatto salvo i documenti per i quali non sussiste competenza delle AOO.

10.5. Registrazione di protocollo

L'operatore di protocollo deve registrare un determinato documento così come è pervenuto. Si tratta dunque di una delicata competenza finalizzata ad accertare la certezza giuridica di data, forma e provenienza per ogni documento.
La registrazione viene effettuata di norma entro 24 ore lavorative decorrenti dalla giornata di arrivo, ad eccezione dei casi in cui è prevista la protocollazione successiva.
Poiché la data di registrazione di un documento è parte integrante della segnatura di protocollo non è necessario apporre al documento stesso altri timbri che riportino l'indicazione della data di ricezione.
L'Ufficio Protocollo provvede alla protocollazione dei documenti utilizzando il sistema informatico Archiflow, di cui al paragrafo 9.
La registrazione dei documenti ricevuti o spediti è effettuata in un'unica operazione.
L'operazione di registrazione può essere di 3 tipi:

- registrazione in Entrata, Uscita;
- registrazione comunicazioni Interne;
- registrazione di emergenza in Entrata, Uscita.

Le registrazioni di protocollo dei documenti ricevuti sono effettuate il giorno della ricezione o comunque entro il giorno successivo, se lavorativo, da parte delle unità di protocollazione abilitate. Il contenuto del registro e del sistema di protocollo informatico è salvato periodicamente su supporti di memorizzazione. Delle registrazioni del protocollo informatico è sempre possibile estrarre evidenza analogica.

10.6. Segnatura di protocollo

L'operazione di segnatura di protocollo è effettuata contemporaneamente all'operazione di registrazione di protocollo.
La segnatura di protocollo è l'apposizione, o l'associazione all'originale del documento, in forma permanente non modificabile, delle informazioni riguardanti il documento.
Essa consente di individuare ciascun documento in modo inequivocabile.
Per la "Posta in entrata cartacea", la segnatura di protocollo apposta o associata al documento è effettuata dall'Ufficio Protocollo con apposito timbro prima della registrazione dei dati nel protocollo informatico.
Per la "Posta in entrata informatica", le informazioni sono apposte automaticamente sul documento informatico dal software del protocollo informatico riportando gli stessi elementi previsti per la segnatura del documento analogico.
Le informazioni che costituiscono la segnatura prevedono:

- il numero di protocollo;
- la data e l'ora di protocollo;
- l'indicazione della tipologia di registrazione (I/U);
- la denominazione dell'Azienda.

10.7. Scansione dei documenti cartacei

I documenti su supporto cartaceo soggetti a registrazione di protocollo – sia in entrata che in uscita – di formato inferiore o uguale ad A4, dopo le operazioni di registrazione, classificazione e segnatura, devono essere acquisiti in formato immagine con l'ausilio di scanner nel formato conforme alla tecnologia in uso.
In alcuni casi, per i documenti voluminosi si acquisirà in formato immagine solo il frontespizio.
Il processo di scansione dei documenti cartacei, al fine di trasformarli in formato immagine, avviene – per i documenti in entrata - nella fase di registrazione del protocollo, a cura dell'Ufficio Protocollo. Per i documenti in uscita, la scansione è operata dall'U.O. che lo produce.
La scansione si articola nelle seguenti fasi:

- acquisizione del documento in modo che, se composto da più fogli, corrisponda ad un unico file in un formato standard idoneo alla conservazione;
- verifica della leggibilità delle immagini acquisite e della loro esatta corrispondenza con gli originali cartacei.

10.8. Documenti soggetti a protocollo riservato

Tutti i documenti vengono registrati utilizzando il protocollo informatico unico dell'Arnas.
Nei casi in cui sia necessario adottare misure di riservatezza ulteriori (ad esempio, nei casi seguenti: documenti legati a vicende di persone o a fatti privati, documenti contenenti informazioni sensibili, documenti dalla cui contestuale pubblicità possa derivare pregiudizio a terzi o al buon andamento dell'attività amministrativa ecc.) nell'oggetto del documento si indicano le generalità degli individui coinvolti utilizzando le iniziali del nome e del cognome anziché riportarle per esteso.
Nel caso di mail (PEC/PEO) in uscita , l'eventuale file allegato deve essere rinominato con la dicitura "Documento Riservato", la stessa dicitura riportata nell'oggetto della Mail.
In caso di ricezione di documento riservato, in fase di protocollazione, se non già presente, si integra l'oggetto con la dicitura "protocollo riservato" e si assegna al destinatario interno competente togliendo la visibilità a tutte le altre strutture ad eccezione della Direzione Generale.

10.9. Annullamento delle registrazioni di protocollo

Il sistema di protocollo informatico non consente di annullare le registrazioni di protocollo.

10.10. Chiusura delle attività di protocollo

Al fine di assicurare l'integrità e la disponibilità dei dati contenuti nel registro di protocollo generale delle AOO, in fase di chiusura dell'attività di protocollo, il Sistema provvede ad effettuare le seguenti operazioni:

- creazione di una scheda relativa al documento in Entrata/Uscita o Interno con il

numero generale di protocollo;
- applicazione di un riferimento temporale al file così realizzato;
- archiviazione informatica sui server dell'Arnas.

È inoltre disponibile per gli operatori del SPI una funzione applicativa di "Stampa registro di protocollo" per i propri usi interni.

11. Archiviazione dei documenti analogici

L'archivio è suddiviso funzionalmente in:
- archivio corrente;
- archivio di deposito;
- archivio storico.

Per archivio corrente s'intende il complesso dei documenti relativi ad affari e a procedimenti amministrativi in corso d'istruttoria e di trattazione o comunque verso i quali sussista un interesse corrente; tali documenti sono allocati presso gli uffici della U.O.C. produttrice.
Per archivio di deposito si intende il complesso di fascicoli sanitari e amministrativi relativi ad attività, affari, pratiche e procedimenti amministrativi conclusi, per i quali non risulta più necessaria una trattazione o comunque verso i quali sussista comunque la necessità di consultazione saltuaria. L'ARNAS conserva i propri documenti nell'archivio di deposito affidato ad un terzo con apposito contratto di servizio.
Per archivio storico s'intende il complesso dei documenti relativi ad affari e a procedimenti amministrativi conclusi da oltre 40 anni e destinati, previa l'effettuazione delle operazioni di scarto, alla conservazione perenne nella sezione separata d'archivio presso i locali dell'ARNAS.

12. Piano di conservazione

Lo scarto avviene ai sensi dell'art. 35 del D.P.R. 30.09.1963 n. 1409 e secondo il titolario di scarto allegato al presente Manuale di Gestione.
Lo scarto della documentazione negli archivi pubblici rappresenta un'operazione fondamentale per garantire una gestione efficiente e ordinata. Si tratta della rimozione di quei documenti che non sono più utili per scopi amministrativi o legali e che non presentano un interesse storico rilevante. Questa procedura è regolata dal decreto legislativo 22 gennaio 2004, n. 42, e richiede l'autorizzazione preventiva della Soprintendenza archivistica, come indicato all'articolo 21, comma 1, lettera d).

Pertanto il Responsabile della gestione documentale, prima di poter procedere allo scarto dei documenti in archivio, presenterà una richiesta formale alla Soprintendenza archivistica. La richiesta deve essere accompagnata da un elenco dettagliato dei materiali che si intendono eliminare.
In particolare, l'elenco deve includere:
- Tipologia dei documenti che devono essere individuati con una descrizione chiara, utilizzando la terminologia del Piano di conservazione dell'ente;
- Estremi cronologici ovvero le date di riferimento per ogni tipologia documentaria;
- Il numero di pezzi da eliminare (buste, registri, scatole, metri lineari, ecc.);
- La Motivazione del perché si propone lo scarto.

Successivamente la Soprintendenza, esaminati i documenti può autorizzare lo scarto, in tutto o in parte, oppure respingere la richiesta. Questo procedimento deve essere concluso entro 60 giorni, salvo eventuali richieste di chiarimenti che possono sospendere i termini.
Ricevuta l'autorizzazione, l'Arnas affida i documenti da eliminare alla ditta specializzata e aggiudicataria del servizio di archiviazione, che ne garantisce la distruzione in modo sicuro tramite le procedure standardizzate (invio alla cartiera per la distruzione con rilascio del relativo formulario di avvenuto smaltimento). Particolare attenzione è riservata ai documenti contenenti dati sensibili, per i quali viene rispettata la normativa sulla privacy.

Infine, il Responsabile della gestione documentale trasmette alla Soprintendenza il verbale di avvenuta distruzione, entro 60 giorni dall'eliminazione, per completare formalmente il procedimento.

13. Misure di sicurezza adottate

Conformemente all'art. 51, c. 2 del CAD, l'ARNAS assicura il controllo e la conservazione dei documenti digitali di cui è responsabile, adottando modalità atte a minimizzare il rischio di distruzione, smarrimento, accesso non autorizzato o utilizzo improprio. A tale scopo, l'ICT Management stabilisce misure e tecniche organizzative atte a garantire la sicurezza delle applicazioni e dell'infrastruttura del sistema di protocollo e gestione documentale, assicurando che le informazioni e i documenti archiviati siano accessibili nel rispetto delle normative sulla riservatezza e protezione dei dati personali, mantenendone al contempo integrità, autenticità e leggibilità.

In particolare, queste misure sono finalizzate a garantire ed assicurare:

- la disponibilità, l'integrità e la protezione delle informazioni sensibili, assicurando un adeguato livello di riservatezza;
- l'accessibilità agli atti, ai documenti e ai dati nel rispetto dei principi di privacy e trasparenza dell'operato amministrativo;
- la custodia dei documenti in modo da minimizzare rischi di obsolescenza dei formati, perdite accidentali o distruzione di dati;
- il corretto trattamento dei dati e delle informazioni di cui l'Azienda Ospedaliera è titolare e responsabile.

Inoltre, tra le strategie di sicurezza messe in atto dall'ICT Management per mitigare i rischi derivanti dall'obsolescenza tecnologica e garantire disponibilità, consultabilità e leggibilità nel tempo dei documenti, preservandone l'integrità, vi è l'adozione di formati di file conformi alle direttive contenute nell'Allegato 2 alle LL.GG. AgID.

L'Arnas esegue, inoltre, verifiche periodiche per valutare l'adeguatezza dei formati di archiviazione dei file rispetto agli sviluppi scientifici e tecnologici, prevedendo, se necessario, la migrazione delle informazioni del protocollo informatico su nuovi supporti, in conformità con quanto stabilito dall'art. 62 del D.P.R 445/2000.

L'implementazione di queste misure e la verifica della loro corretta applicazione rientrano tra le responsabilità dell'amministrazione, in qualità di Titolare del trattamento dei dati. In caso di violazione dei dati personali, sono previste la notifica all'autorità di controllo e la comunicazione della violazione agli interessati, ai sensi degli artt. 33 e 34 del Regolamento UE 2016/679.

Nei paragrafi seguenti vengono illustrate le misure di sicurezza informatica in linea con le previsioni del *Piano triennale per l'informatica nella PA* (AgID, 2024-2026), e nel rispetto delle disposizioni di sicurezza stabilite dall'AgID e dagli organismi competenti, delle normative sulla protezione dei dati personali (secondo l'analisi del rischio effettuata) e delle linee guida sulla continuità operativa dei sistemi informatici fornite da AgID.

In particolare, vengono descritte le misure di sicurezza attinenti alle aree indicate di seguito:

- sistema informatico di protocollo;
- continuità operativa del servizio di gestione documentale;
- protezione della riservatezza e dei dati personali;
- controllo degli accessi alle informazioni e monitoraggio attività degli utenti.

13.1. Piano della sicurezza del sistema di protocollo e di gestione documentale

In conformità con le disposizioni previste dalle LL.GG. AgID, l'ICT Management, che ricopre anche il ruolo di Responsabile della conservazione, elabora e adotta il presente Piano della sicurezza per il sistema di protocollo e la gestione documentale. Tale piano prevede l'implementazione di misure tecniche e organizzative adeguate, al fine di garantire un livello di sicurezza proporzionato ai rischi legati alla protezione dei dati personali, in conformità con l'art. 32 del Regolamento UE 2016/679, e in relazione alle tipologie di dati trattati, inclusi quelli appartenenti a categorie particolari ai sensi degli artt. 9 e 10 dello stesso Regolamento.

Il sistema di protocollo attualmente operativo integra funzionalità che garantiscono la conformità alle disposizioni in materia di sicurezza e tutela dei dati personali. Nello specifico, queste assicurano:

- l'univoca identificazione ed autenticazione degli utenti;
- l'accesso alle risorse riservato esclusivamente a utenti autorizzati e/o a gruppi definiti attraverso specifici profili applicativi (Ruoli applicativi);
- la registrazione permanente di qualsiasi modifica effettuata sulle informazioni trattate, consentendo la tracciabilità e l'attribuzione delle responsabilità.

Ai sensi dell'art. 52 del D.P.R. 445/2000, vengono garantite inoltre:

- sicurezza e integrità;
- corretta e puntuale registrazione dei documenti e loro organizzazione nell'ambito del sistema di classificazione d'archivio adottato;
- reperimento delle informazioni riguardanti i documenti registrati;

- accesso in condizioni di sicurezza alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di tutela della privacy.

Infine, ai sensi dell'art. 58, c. 3, del D.P.R. 445/2000, il sistema consente l'elaborazione di statistiche sulle informazioni registrate, supportando così le attività di controllo e monitoraggio.

13.1.1. Criteri di accesso al sistema da parte del personale interno ed esterno

L'accesso al sistema di protocollo e di gestione documentale da parte degli utenti appartenenti all'Amministrazione è direttamente raggiungibile via Internet e non vi è la necessità di instaurare un tunnel VPN. L'autenticazione avviene direttamente tramite il portale, che espone un endpoint accessibile da qualsiasi dispositivo connesso alla rete, sia da postazioni interne all'ente che da ubicazioni remote, inclusi accessi da rete domestica. Questo modello consente maggiore flessibilità operativa, eliminando la dipendenza da infrastrutture VPN, ma introduce al contempo considerazioni aggiuntive in termini di sicurezza, come la necessità di meccanismi avanzati di protezione degli endpoint esposti su rete pubblica (es. firewall applicativi e sistemi di autenticazione robusti).
Il controllo degli accessi è assicurato da un sistema di autorizzazione basato sulla *profilazione preventiva degli utenti*, che consente di definire l'insieme delle abilitazioni, delle autorizzazioni e dei permessi associati a ciascuno di essi, al fine di impedire accessi non autorizzati alla documentazione e di circoscrivere le operazioni effettuabili sui dati e sui documenti.
Per l'abilitazione di soggetti esterni all'Amministrazione, identificabili, ad esempio, nei fornitori e nei consulenti che forniscono supporto all' Azienda nello svolgimento delle attività e delle funzioni amministrative, è prevista la medesima procedura sopra descritta per l'abilitazione del personale interno.

13.1.2 Funzioni di tracciamento e monitoraggio

Il sistema di protocollo e di gestione documentale dispone di specifiche funzionalità per il monitoraggio e la storicizzazione delle operazioni effettuate all'interno dello stesso. In particolare, tali funzioni garantiscono:

- Il tracciamento delle singole operazioni svolte dagli utenti;
- Il mantenimento, all'interno del sistema, di tutti i dati di rilevamento delle attività e delle operazioni effettuate dagli utenti, secondo modalità sicure tali da non consentire modifiche non autorizzate;
- Il controllo degli accessi al sistema ed alla documentazione in esso registrata.

13.1.3 Manutenzione ordinaria, aggiornamenti e interventi evolutivi

Allo scopo di garantire la sicurezza della componente logica e fisica del sistema, è prevista una manutenzione ricorrente, finalizzata a preservare la piena funzionalità del sistema e a ridurre al minimo le possibili alterazioni.
L'aggiornamento della versione del *software* è previsto sia in caso di variazioni di carattere normativo, dalle quali deriva la necessità di effettuare interventi adeguativi, sia in caso di interventi evolutivi richiesti dal responsabile per l'implementazione di nuove funzionalità. Nella prima casistica rientra, ad esempio, l'intervento di aggiornamento del *software* a seguito dell'entrata in vigore delle LL.GG. AgID nel gennaio 2022, che ha riguardato lo

sviluppo e l'implementazione di specifiche funzionalità volte a garantire la conformità ai requisiti di legge in termini di:
• Definizione dei metadati (Allegato 5 alle LL.GG. AgID);
• Interoperabilità via PEC e via Web Services (Allegato 6 alle LL.GG. AgID);
• Revisione delle procedure per la storicizzazione delle modifiche dei dati.

13.1.4 Continuità operativa

Per garantire la continuità operativa del sistema e delle operazioni indispensabili per i servizi erogati, in caso di emergenza o di aggiornamento del *software* sono previste determinate procedure di salvataggio dei dati e specifiche funzionalità per la registrazione dei documenti. Inoltre, sono previste procedure volte ad assicurare il ritorno alla normale operatività del sistema e il recupero dei dati al termine della fase di emergenza.

13.2. Criteri di accesso ai dati, ai documenti e alle funzionalità del sistema

L'accesso ai dati, ai documenti e alle funzionalità del sistema di protocollo e di gestione documentale è regolato da criteri basati su specifiche *policy* di visibilità e sulla profilazione preventiva degli utenti, di seguito riportate.

13.2.1 Policy di visibilità dei dati e dei documenti

Le *policy* di visibilità implementate nel sistema sono riconducibili sia ai parametri di autorizzazione definiti dall'ICT Management, sia a funzionalità di base configurate in base alle disposizioni di legge su diritto di accesso e tutela della riservatezza.
In particolare, la visibilità dei dati e dei documenti è determinata da:

- Logiche di visibilità gerarchica;
- Criteri di abilitazione all'accesso, da parte degli utenti, alla documentazione registrata sul Registro ufficiale di protocollo della AOO, sui Repertori interni o su altri eventuali registri;
- Liste di competenza (Access Control List – ACL);
- Flussi di assegnazione dei documenti e dei fascicoli.

Le logiche di visibilità gerarchica impostate di *default* nel sistema garantiscono alle strutture organizzative dell'ARNAS di accedere ai dati e di controllare le attività svolte dalle strutture sottostanti. Viceversa, è inibita la possibilità da parte degli uffici di livello gerarchico inferiore di accedere a dati e documenti gestiti dalle strutture superordinate.
Per quanto invece riguarda i criteri di abilitazione di accesso alla documentazione nel Registro ufficiale di protocollo, questi sono volti ad assicurare la visibilità dei dati e dei documenti registrati nel sistema ai soli soggetti autorizzati.
Le Liste di competenza sono utilizzate per definire gli utenti/uffici da abilitare alla consultazione e all'operatività su determinate aggregazioni documentali, circoscrivendone quindi l'accesso ai soli soggetti autorizzati.
Infine, un altro importante criterio di regolamentazione delle visibilità dei dati e dei documenti di cui l'Amministrazione è titolare e depositaria è rappresentato dai flussi di assegnazione che consentono, di estendere temporaneamente la visibilità e parte dell'operatività sui documenti e sui fascicoli agli utenti/uffici non abilitati, secondo i criteri sopradescritti, in base a specifiche necessità.

13.2.2 Profilazione preventiva degli utenti

La *profilazione preventiva degli utenti* è regolata dai Ruoli applicativi, funzionalità del sistema di protocollo e di gestione documentale che consentono di definire permessi e autorizzazioni da associare agli utenti, al fine di circoscrivere il perimetro delle funzionalità e delle operazioni consentite a questi ultimi su dati e documenti registrati nel sistema stesso.
A ciascun utente, inoltre, può essere associato più di un Ruolo applicativo e, nel caso in cui lo stesso appartenga a più uffici, viene fornita la possibilità di selezionare il Ruolo attraverso il quale operare in ciascun ufficio.
Le attività di configurazione dei Ruoli applicativi sono di competenza degli utenti in possesso del Ruolo di Amministratore di sistema e sono regolate da criteri organizzativi e autorizzativi interni all'Amministrazione.

13.2.3 Accesso alla documentazione riservata e contenente dati sensibili

Ai sensi dell'art. 32 del *Regolamento* UE 2016/679, l'Amministrazione, tenendo conto dei rischi che derivano dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, ai dati personali di cui è titolare e depositaria, mette in atto adeguate misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio, che comprendono:

- la pseudonimizzazione e la cifratura dei dati personali;
- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza

dei sistemi e dei servizi di trattamento;

- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di

incidente fisico o tecnico;

- procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Tali misure sono garantite dal ricorso a specifiche funzionalità del sistema di protocollo che consentono una corretta gestione della documentazione riservata e contenente dati personali. In particolare, per la gestione dei documenti contenenti dati sensibili il sistema mette a disposizione una funzionalità attivabile in fase di protocollazione, che consente sia di impedirne l'accesso agli utenti non abilitati o non opportunamente autorizzati.
Appartengono a tale categoria:

- i documenti relativi a vicende di persone fisiche o giuridiche, o a fatti privati particolari;
- i documenti di indirizzo e di carattere politico che, se resi di pubblico dominio, possono ostacolare il

raggiungimento degli obiettivi prefissati;

- i documenti dalla cui contestuale pubblicità possa derivare pregiudizio a terzi o al buon andamento dell'attività amministrativa;
- i documenti individuati ai sensi dell'art. 24 della l. 241/1990;
- i documenti individuati ai sensi del d.lgs. 30 giugno 2003, n. 196 (con particolare riferimento all'art. 102) e della l. 124/2007.

Questa tipologia è circoscritta ai soli utenti abilitati dall'Amministrazione che nel sistema di protocollo dispongono di determinati permessi applicativi, che consentono di utilizzare funzionalità dedicate.

ALLEGATO 1

REGISTRO DI EMERGENZA

Nel caso di inconvenienti tecnici che dovessero protrarsi oltre le 48 ore sui collegamenti telematici o comunque sul funzionamento del sistema di protocollo, su disposizione del Direttore Generale, potrà essere attivata la procedura di emergenza, mediante ricorso ad operazioni di registrazione manuale.

Per attivare il registro di protocollo di emergenza si deve verificare almeno una delle seguenti condizioni:

1) guasto al software di protocollazione informatica;

2) guasto al sistema informatico di gestione;

3) mancanza di energia elettrica.

Qualora una di queste condizioni si protraesse oltre le 48 ore, è attivato il Registro di protocollo di emergenza su supporto cartaceo, registro predisposto secondo l'allegato fac-simile (modulo 3) e soggetto a periodo di conservazione permanente.

La gestione del protocollo di emergenza per le AOO, comporterà la protocollazione sia in entrata che in uscita.

Per l'attivazione del protocollo di emergenza il Direttore Generale dovrà:

1) redigere il verbale di attivazione (modulo n. 1);

2) comunicare agli assetti aziendali l'attivazione dell'emergenza;

Sul "Protocollo di Emergenza" dovranno essere riportate le seguenti informazioni necessarie:

- numero progressivo di Protocollo di emergenza;
- data di protocollazione;
- tipo di protocollo (Entrata, Interno, Uscita -"E", "I, "U");
- oggetto;
- mittente;
- destinatario;
- classificazione del documento;
- rif. documento;
- data rif. documento;
- n. eventuali allegati;

Potranno essere inoltre riportate le seguenti informazioni accessorie:

- eventuali note;
- tipo di documento (lettera, raccomandata A/R, fax, ecc...);

A ciascun documento registrato in emergenza dalla AOO andrà attribuito, per ciascun anno solare, un numero progressivo a partire da 1, preceduto dalla dicitura “Prot EM”.

Esempio: Prot. EM. n° 1 del gg/mm/aaaa

Sui documenti registrati in emergenza presso le AOO, la dicitura Prot.EM. sarà seguita

dall' idonea sigla identificativa:

- Direzione Aziendale - DA;
- Servizio Risorse Umane - ARU;
- Provveditorato Economato - APE;
- Affari Generali - AAGG;
- Servizio Tecnico - TEC;

Esempi: Prot. EM./DA n° 1 del gg/mm/aaaa, Prot. EM./AAGG n° 1 del gg/mm/aaaa

La numerazione di ciascun registro di emergenza è unica per l'intero anno. Ricomincia dal numero successivo all'ultimo utilizzato per ogni attivazione.

Al termine dell'emergenza, il Responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi dovrà:

a) revocare l'autorizzazione alla protocollazione di emergenza (modulo n. 2);

b) comunicare agli assetti aziendali la revoca dell'emergenza;

c) comunicare alla Soprintendenza Archivistica il ripristino delle funzionalità del registro di protocollo informatico.

Una volta riattivato il sistema informatico, gli Uffici incaricati della gestione dell'emergenza dovranno procedere alla ri-protocollazione dei documenti mediante l'applicativo informatico: nel campo "oggetto" dovrà essere riportato il numero di Protocollo di Emergenza già attribuito al documento e la relativa data (Es.: Prot. EM./DGD 1 n° 1 del gg/mm/aaaa); ciò permetterà di conservare traccia di tutta la protocollazione aziendale registrata in emergenza, consentendone una futura reperibilità anche attraverso il sistema informatico.

Modulo n.1

AUTORIZZAZIONE ALLO SVOLGIMENTO DELLE OPERAZIONI
DI REGISTRAZIONE DI PROTOCOLLO SUL REGISTRO DI EMERGENZA (art. 63 DPR 445/2000)

Ai sensi dell'art. 63 del DPR 28 dicembre 2000 n. 445:

- preso atto che, per le cause sotto riportate:

Data interruzione	
Ora interruzione	
Causa della interruzione	

non è possibile utilizzare la normale procedura informatica;

- si autorizza lo svolgimento delle operazioni di registrazione di protocollo sul Registro di emergenza.

IL DIRETTORE GENERALE

Modulo n.2

REVOCA AUTORIZZAZIONE ALLO SVOLGIMENTO DELLE OPERAZIONI DI REGISTRAZIONE DI PROTOCOLLO SUL REGISTRO DI EMERGENZA (art. 63 DPR 445/2000)

Ai sensi dell'art. 63 del DPR 28 dicembre 2000 n. 445:

- ricordato che, per le cause sotto riportate:

Data interruzione	
Ora interruzione	
Causa della interruzione	

- non essendo possibile utilizzare la normale procedura informatica, è stato autorizzato lo svolgimento delle operazioni di registrazione di protocollo sul Registro di emergenza;
- preso atto che, dalla data ed ora sotto riportate:

Data di ripristino	
Ora di ripristino	

è stato ripristinato il normale funzionamento della procedura informatica;

- si revoca l'autorizzazione allo svolgimento delle operazioni di registrazione di protocollo sul Registro di emergenza;
- si dispone il tempestivo inserimento delle informazioni relative ai documenti protocollati in emergenza nel sistema informatico, con automatica attribuzione della numerazione di protocollo ordinaria, mantenendo la correlazione con la numerazione utilizzata in emergenza.

IL DIRETTORE GENERALE

Modulo n.3

REGISTRO DI EMERGENZA

AOO _____

Numero Registrazione emergenza	Data	Tipo E - I- U	Mittente	Destinatario	Oggetto	Classificazione Titolario/n. Fascicolo	N All

ALLEGATO 2

Il *Piano di conservazione -Titolario di classificazione e Massimario di scarto -*

Premessa

Il Piano di conservazione -Titolario di classificazione e Massimario di scarto - della documentazione sanitaria, sociosanitaria e amministrativa sono stati redatti dall'Arnas in collaborazione con la Soprintendenza archivistica per la Sicilia , così come auspicato dal Decreto legislativo n. 42/2004 "Codice dei beni culturali e del paesaggio".

Tale progetto nasce dall'esigenza di dotare l'azienda di uno strumento di riferimento, che possa migliorare la qualità e la sicurezza dell'assistenza sanitaria e tutelare il patrimonio documentale.

La documentazione sanitaria testimonia gli eventi e le attività che si verificano durante i processi di assistenza. La memoria documentale costituisce un bene di straordinaria importanza sul piano clinico, scientifico e didattico, oltre che giuridico, sia per il cittadino, che se ne può servire per far valere i propri diritti, sia per la tutela dell 'operato professionale degli operatori sanitari.

Gestire correttamente la documentazione sanitaria, sulla base di dati aggiornati e puntuali, contribuisce a integrare e a dare coerenza alle decisioni dei molteplici attori coinvolti nei processi di assistenza e ad accrescere la sicurezza del paziente.

Il Titolario di classificazione è lo schema logico utilizzato per organizzare i documenti d'archivio in base alle funzioni e alle materie di competenza dell'azienda.

Il titolo individua per lo più funzioni primarie e di organizzazione dell'azienda (macrofunzioni); le successive partizioni, classi e sottoclassi, corrispondono a specifiche competenze che rientrano concettualmente nella macrofunzione descritta dal titolo, articolandosi gerarchicamente tra loro in una struttura ad albero rovesciato.

Il Titolario si suddivide, di norma, in titoli, classi, sottoclassi, categorie e sottocategorie o, più in generale, in voci di I livello, II livello, III livello.

La classificazione dei documenti ha lo scopo di realizzare una corretta organizzazione dei documenti nell'archivio del sistema del protocollo informatico e si avvale del cosiddetto "Titolario", che rappresenta un sistema precostituito di partizioni astratte gerarchicamente ordinate, individuato sulla base dell'analisi delle attività connesse all'organizzazione aziendale, al quale viene ricondotta la molteplicità dei documenti prodotti.

Il titolario è soggetto ad aggiornamento in ragione della dinamica organizzativa dell'Azienda e deve garantire la storicizzazione delle sue variazioni, con 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. L'aggiornamento del piano di classificazione avviene con provvedimento del Direttore Generale.

Il Massimario di scarto intende fornire le indicazioni utili per la corretta e ordinata tenuta e gestione degli archivi aziendali in ottemperanza agli obblighi di legge in materia di conservazione dei documenti prodotti e acquisiti dall'Azienda nello svolgimento della propria attività istituzionale.

Il presente atto definisce, altresi, la procedura per la preparazione e selezione dei suddetti documenti al fine dello scarto.

Per quanto non espressamente previsto dal presente atto si fa riferimento alle disposizioni della vigente normativa di settore.

Per Massimario di conservazione e di scarto si intende l'elenco della tipologia dei documenti con il rispettivo tempo di conservazione (limitato o illimitato).

Il Massimario è uno strumento di ausilio per gestire in modo organizzato un archivio, permettendo di conservare solo quello che mantiene un rilievo giuridico o ha assunto un valore storico e di eliminare la documentazione giudicata non più utile.

Prima di procedere a qualsiasi scarto in applicazione del massimario, è opportuna una verifica attenta del contenuto della documentazione da eliminare per non distruggere dati acquisiti nel tempo in campo sanitario ed amministrativo che potrebbero in futuro rivelarsi utili non solo ai fini della salute pubblica e del privato cittadino, ma anche per contribuire alla valorizzazione del patrimonio storico-culturale.

Al fine di pervenire ad una maggiore omogeneità tra i servizi nella gestione dei documenti e dei relativi tempi di conservazione si è provveduto a predisporre un Massimario-Prontuario.

Lo scarto rappresenta lo strumento per gestire in maniera ordinata un archivio corrente e di deposito: esso è un elemento qualificante dell'archivio stesso, in quanto permette di conservare solo ciò che, terminato il periodo di valenza amministrativa e legale, ha assunto un valore storico e consente di eliminare la documentazione giudicata superflua.

L'eliminazione della documentazione inutile presuppone una conduzione ordinata e razionale dell'archivio fin dall'inizio. Occorre essere costantemente aggiornati sui documenti che si producono e si ricevono, classificandoli per dare loro un ordine logico e per facilitare al massimo il loro reperimento in archivio, programmare fin dall'inizio i loro tempi di conservazione, procedere alla eliminazione periodica degli atti inutili

A tale scopo si rende indispensabile uno strumento capace di vagliare e selezionare tutti i documenti, evitando di mantenere una raccolta casuale di carte che occupa uno spazio vitale e nella quale la ricerca e l'estrazione di un documento sono affidate al caso.

Il Massimario è in grado di fornire il mezzo per permettere all'azienda di liberarsi periodicamente di carte superflue senza correre il rischio di distruggere documenti di importanza storica. Esso è lo strumento di una gestione corretta di un archivio, ultimo anello della catena gestionale che comincia con la protocollazione, prosegue con la razionale classificazione dell'archivio corrente e continua con l'ordinata immissione nell'archivio storico dei documenti a conservazione illimitata.

Vedi allegato esterno

ALLEGATO 3

Manuale di conservazione dei Documenti informatici

Vedi allegato esterno

ALLEGATO 4

Nomina del DPO e altre nomine

Vedi allegato esterno

ALLEGATO 5

Regolamento per l’esercizio del diritto all’accesso civico

Vedi allegato esterno