Linee Guida per la Classificazione delle Informazioni e dei Trattamenti

Autore/i:	Annalisa Cocco	Cybermind S.r.l.
Rivisto Da	Vitagliozzi Alessandra	Cybermind S.r.l.
Approvato Da:	Carmine Maraio, Helga Fineo	Sistemi Informativi S.p.A., IBM S.p.A.
Accettato Da:	Alberto Genovese	So.Re.Sa. S.p.A.

Storia del documento

Data	Versione	Descrizione modifiche	Autore

Sommario

1 Generalità

1.1 Finalità del documento

Il presente documento descrive le regole adottate dalla Struttura Sanitaria, per la gestione delle informazioni e dei trattamenti classificati, con particolare riguardo ai dati personali ai sensi del GDPR [1].

Obiettivo della presente Linea Guida è quello di indirizzare la tutela delle informazioni relative ai dati personali trattate dalla Struttura Sanitaria, al fine di proteggerle a prescindere dall'origine, dal supporto o dalla fase di elaborazione.

Le linee guida descritte all'interno del presente documento sono da considerarsi misure minime la cui attuazione si rende necessaria per contenere, entro limiti accettabili, il rischio di compromissioni della riservatezza, integrità e disponibilità delle informazioni e dei trattamenti di dati personali effettuati dalla Struttura Sanitaria.

In tal senso, queste costituiscono i requisiti di base che devono essere rispettati e che, in quanto tali, in virtù delle specifiche caratteristiche del contesto operativo cui si applicano possono essere incrementati nei casi in cui siano richiesti livelli di protezione più elevati.

1.2 Ambito di applicazione

Gli indirizzamenti definiti nel presente documento si applicano a:

- i trattamenti di dati personali ai sensi del GDPR [1] effettuati presso la Struttura Sanitaria;
- tutti gli asset a supporto dei suddetti trattamenti.

Si precisa inoltre che la classificazione delle informazioni oggetto di questo documento si riferisce esclusivamente alla salvaguardia dei diritti e delle libertà dell'interessato ai sensi del GDPR [1], non intende quindi trattare principi come il segreto di stato o il segreto professionale, oggetto di normative diverse.

1.3 Documenti di riferimento

[1] Regolamento (UE) 2016 del Parlamento Europeo e del Consiglio, del 27 Aprile 2016, relativo alla protezione delle persone con riguardo al trattamento dei dati personali – Regolamento Generale sulla Protezione dei Dati (GDPR) e s.m.i.

[2] D.lgs 10 agosto 2018, n. 101. “Disposizioni per l’adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)” e s.m.i.

[3] D.Lgs. 30 Giugno 2003, n. 196 “Codice in materia di protezione dei dati personali” e s.m.i.

[4] “Linee guida in materia di Dossier sanitario” del Garante per la protezione dei dati personali del 4 giugno 2015 (G.U. n. 164 del 17 luglio 2015)

[5] D. lgs 24 Gennaio 2006, n.36 “Attuazione della direttiva 2003/98/CE relativa al riutilizzo di documenti nel settore pubblico” e s.m.i.

[6] ISO/IEC 27001:2013 “Information Security Management Systems”, 01/10/2013

[7] ISO/IEC 27002:2013 “Code of practice for information security controls", 01/10/2013

[8] ISO/IEC 27001:2017 “Information technology — Security techniques — Information security management systems - Requirements”, 2017-03

[9] Lg. 124 del 2007 "Sistema di informazione per la sicurezza della Repubblica"

[10] DPCM 6 novembre 2015, n. 5, "Disposizioni per la tutela amministrativa del segreto di Stato e delle informazioni classificate e a diffusione esclusiva"

[11] Politica per la Cancellazione Sicura e lo Smaltimento dei Supporti Elettronici della Struttura Sanitaria

[12] Politica per il corretto utilizzo delle risorse informative aziendali della Struttura Sanitaria

[13] Allegato 1 al Provvedimento del Garante per la protezione dei dati personali N. 467 dell’11 Ottobre 2018: Elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d’impatto

[14]

1.4 Acronimi e definizioni

Termine	Definizione
Banca dati	Qualsiasi complesso organizzato di dati (archivio informatico), riguardanti uno stesso argomento o più argomenti correlati tra loro, strutturato in modo tale da consentire la gestione dei dati stessi (l'inserimento, la ricerca, la cancellazione ed il loro aggiornamento) da parte di un applicazione, ripartito in uno o più elaboratori elettronici (ad es. server, postazioni lavorative, ecc.) dislocati all'interno della rete LAN della Struttura Sanitaria.
Classificazione	L'attribuzione all'informazione di un livello di classificazione ovvero il suo inserimento all'interno di una classe di sicurezza.
Cancellazione sicura	Modalità di cancellazione che consiste nell'eliminazione irreversibile dei dati contenuti in un supporto elettronico in modo che essi non siano più accessibili a terzi o risultino comunque inintelligibili impedendo così il recupero degli stessi.
Categorie particolari di dati personali	Ai sensi dell'art. 9 del regolamento (UE) 2016/679 - GDPR [1]: Dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
Dato	L'informazione puntuale contenuta in un archivio cartaceo o informatico.
Dati personali relativi a condanne penali e reati	Ai sensi dell'art. 10 del regolamento (UE) 2016/679 - GDPR [1]: Dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza.
Dato personale	Ai sensi dell'art. 4 del regolamento (UE) 2016/679 - GDPR [1]: Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata,

Termine	Definizione
	direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
Dati genetici	I dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.
Dati biometrici	I dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.
Dati ultrasensibili	Dati personali (ai sensi dell'art. 4 del GDPR [1]) soggetti a particolari vincoli di segretezza: dati relativi ad atti di violenza sessuale o di pedofilia, all'infezioni da HIV o all' uso di sostanze stupefacenti, di sostanze psicotrope e di alcool, alle prestazioni erogate alle donne che si sottopongono ad interventi di interruzione volontaria della gravidanza o che decidono di partorire in anonimato e ai servizi offerti dai consultori familiari.
Declassificazione	La soppressione di qualsiasi menzione di classificazione.
Destinatario	La persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati 4.5.2016 IT Gazzetta ufficiale dell'Unione europea L 119/33 membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle

Termine	Definizione
	norme applicabili in materia di protezione dei dati secondo le finalità del trattamento.
Documento cartaceo	L'insieme aggregato di informazioni su supporti cartacei.
Documento elettronico	L'insieme aggregato di informazioni su supporti informatici, ovvero file generati attraverso l'utilizzo delle applicazioni della Struttura Sanitaria (ad es. excel, word, access, ecc.).
GDPR	Regolamento UE n. 679/2016 – General Data Protection Regulation (Regolamento Generale per la Protezione dei Dati) [1]
Informazione	La rappresentazione di dati, atti o fatti rilevanti per la Struttura Sanitaria.
Riclassificazione	La ridefinizione del livello di classificazione attribuito all'informazione e, quindi, lo spostamento all'interno di un'altra classe di sicurezza.
Trattamento	Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Tabella 1 – Acronimi e definizioni

1.5 Ruoli e responsabilità

Ciascun dipendente della Struttura Sanitaria coinvolto nell'applicazione della presente Linea Guida, ha l'obbligo di segnalare al Direttore Generale/DPO eventuali scostamenti rispetto a quanto indicato o qualsiasi caso non espressamente affrontato dalle linee guida di seguito definite, o che si presti a dubbi o mal interpretazioni.

Ogni violazione delle norme sopra indicate può comportare provvedimenti sia in ambito disciplinare che giuridico. In caso di illecito, la Struttura Sanitaria si riserva la facoltà di attivare ogni

misura volta a tutelare le risorse informative della Struttura Sanitaria, in linea con quanto stabilito dalla normativa vigente.

Le funzioni aziendali della Struttura Sanitaria sono responsabili, in base alle specifiche competenze, dell'implementazione dei requisiti individuati all'interno del presente documento, finalizzati alla protezione delle informazioni classificate.

In particolare, sono identificati i seguenti ruoli e responsabilità:

- **Responsabile della classificazione** - la persona responsabile del processo, del progetto o dell'unità organizzativa che produce le informazioni. Tale ruolo prevede le seguenti responsabilità:
  - decidere il livello di classificazione delle informazioni;
  - comunicare il livello di classificazione quando l'informazione è rilasciata o fornita ad un'altra entità;
  - specificare/applicare controlli e misure per proteggere i dati in base al relativo livello di classificazione;
  - definire l'uso e i diritti di accesso alle informazioni nel rispetto del principio del "need to know";
  - educare gli utenti all'uso appropriato e alla protezione dei dati (ad es. awareness);
- **Utilizzatore dell'informazione** - la persona che ha bisogno di accedere a dati/informazioni per svolgere attività relative alle sue mansioni lavorative. L'Information User è responsabile di:
  - trattare i dati/informazioni in base al livello di classificazione stabilito;
  - informare immediatamente il proprietario delle informazioni nel caso in cui ritenga di aver ricevuto informazioni errate.

2 Principi generali

Il modello adottato dalla Struttura Sanitaria non include le informazioni classificabili come "Pubbliche", vale a dire informazioni destinate al pubblico dominio, non sottoposte a vincoli normativi (ad es. applicazione del Regolamento UE n. 679/2016 [1] e del D.Lgs. 101/2018 [2]). Tali informazioni possono essere divulgate al di fuori della Struttura Sanitaria a qualsiasi entità esterna (ad esempio agenzie di stampa, media, istituzioni pubbliche, siti Web di Internet) senza causare alcun danno ai diritti e alle libertà dell'interessato e pertanto sono conoscibili/acquisibili da un qualsiasi cittadino attraverso l'ordinaria diligenza senza necessità di requisiti per l'accesso (ossia identificazione e autenticazione) ed il successivo trattamento (autorizzazione).

Rientrano in questa categoria ad esempio, la documentazione presente in registri pubblici o liberamente scaricabile da Internet, i dati di contatto (indirizzo di posta elettronica, numero di telefono, ecc.) pubblicati sui siti o sulla documentazione rilasciata al pubblico, i dati personali contenuti nei bandi di gara, ecc.

Di conseguenza, le informazioni pubbliche possono essere trattate dalla Struttura Sanitaria senza necessità di essere classificate e quindi possono:

- circolare liberamente nell'ambito della Struttura;
- essere acquisite e trattate senza necessità di autorizzazioni dal personale interno o da terze parti.

3 Classificazione delle informazioni

Tutte le informazioni riguardanti una persona fisica identificata o identificabile (interessato) trattati della Struttura Sanitaria devono essere classificate sulla base dei livelli incrementali descritti nella seguente tabella.

Livelli di classificazione	Descrizione
Uso interno	Dati personali (ai sensi dell'art. 4 del GDPR [1]) a cui tutti i dipendenti della Struttura Sanitaria possono accedere e che possono causare effetti indesiderati se disponibili al pubblico. Le informazioni classificate ad *Uso Interno* possono essere divulgate al di fuori della Struttura Sanitaria rispettando il principio del "need to know ". Rientrano in questa categoria esclusivamente: • dati di contatto dei dipendenti della Struttura Sanitaria e di terze parti; • disposizioni organizzative della Struttura Sanitaria.
Confidenziale	Dati personali (ai sensi dell'art. 4 del GDPR [1]), ad esclusione di quelli già compresi negli altri livelli di classificazione, destinati ad un uso aziendale limitato. L'uso improprio di tali informazioni e la loro divulgazione al di fuori dei destinatari previsti possono causare danni limitati alle libertà e ai diritti degli interessati. Le informazioni possono essere divulgate a entità esterne solo nell'ambito di obblighi contrattuali di riservatezza. Rientrano in questa categoria ad esempio l'anagrafica degli assistiti, dati di contatto degli assistiti, disposizioni disciplinari dei dipendenti.

Livelli di classificazione	Descrizione
Strettamente confidenziale	Dati personali (ai sensi dell'art. 4 del GDPR [1]) tipicamente destinati esclusivamente a singole persone. È probabile che l'uso improprio e la divulgazione al di fuori del personale previsto causino danni significativi alle libertà e ai diritti degli interessati. Queste informazioni sono normalmente esenti dalla divulgazione a enti terzi. Tuttavia, qualsiasi divulgazione a entità esterne deve avvenire in base a stretti obblighi contrattuali di riservatezza (Non Disclosure Agreement) nell'ambito del contratto e in conformità con la norma. Rientrano in questa categoria: • Dati personali particolari (ai sensi dell'art. 9 del GDPR [1]): quelli che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona; • Dati personali relativi a condanne penali e reati (ai sensi dell'art. 10 del GDPR [1]): quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato. • Dati personali (ai sensi dell'art. 4 del GDPR [1]) soggetti a particolari vincoli di segretezza (dati "ultrasensibili"): dati relativi ad atti di violenza sessuale o di pedofilia, all'infezioni da HIV o all' uso di sostanze stupefacenti, di sostanze psicotrope e di alcool, alle prestazioni erogate alle donne che si sottopongono ad interventi di interruzione volontaria della gravidanza o che decidono di partorire in anonimato e ai servizi offerti dai consultori familiari.

Tabella 2 – Livelli di classificazione

Le informazioni classificate riservate secondo i criteri di segretezza della Lg. 124 del 2007 [9] e al DPCM 6 novembre 2015, n. 5 [10], dovranno essere trattate in conformità a tali normative rispettando le regole di tutela da queste previste ed esulano quindi da quanto definito nel presente documento.

3.1 Assegnazione del livello di classificazione

L'assegnazione del livello di classificazione deve essere effettuata nel momento in cui l'informazione viene generata tenendo conto della preclassificazione adottata della Struttura Sanitaria (Allegato 1 – Preclassificazione delle informazioni). Nel caso in cui l'informazione generata non sia presente nella lista di preclassificazione, il livello di classificazione deve essere assegnato in funzione della tipologia dell'informazione stessa, secondo la Tabella 2 – Livelli di classificazione.

Se le informazioni costituiscono un insieme aggregato (ad es. un documento cartaceo o informatico, oppure una banca dati), a questo deve essere attribuito come minimo il livello di classificazione assegnato all'informazione che presentala il livello più elevato.

Un'informazione che riprenda il contenuto di un'informazione classificata deve essere classificata nello stesso grado.

Il livello di classificazione dell'informazione deciso dal Responsabile della Classificazione deve essere mantenuto nel tempo solo per la durata necessaria e non può essere modificato dai soggetti destinatari della stessa, così come il livello attribuito ad un documento (cartaceo o informatico) o ad una banca dati.
Nel caso di trattamento di informazioni non classificate, il Responsabile della classificazione a cui tali informazioni afferiscono è tenuto a provvedere senza ulteriori ritardi alla loro classificazione, in modo tale da recepire i relativi requisiti di sicurezza da applicare.

3.2 Riclassificazione o declassificazione delle informazioni

L'informazione può essere riclassificata o declassificata unicamente con l'autorizzazione scritta del Responsabile della classificazione che ha provveduto alla classificazione.
In caso di urgenza, l'autorizzazione può essere concessa verbalmente, con conferma appena possibile per iscritto.
Allo stesso modo può essere riclassificato o declassificato anche il documento o la banca dati.
La riclassificazione o la declassificazione deve essere portata a conoscenza dei destinatari dell'informazione i quali sono, a loro volta, tenuti ad informarne i destinatari delle eventuali successive trasmissioni.

In alcuni casi, il termine a partire dal quale la documentazione cartacea o informatica può essere riclassificata o declassificata, può essere legato a tempi di conservazione dettati da specifiche direttive della Struttura Sanitaria, esigenze normative o legate alla mission della Struttura.

3.3 Etichettatura delle informazioni

Il livello di classificazione delle informazioni deve essere ben noto a tutto il personale dipendente o Enti terzi operanti per la Struttura Sanitaria. A tal fine la Struttura Sanitaria deve diffondere la preclassificazione delle informazioni e le modalità di trattamento associate ai vari livelli, enunciate nella presente linea guida.

Nel caso in cui fosse possibile (per es. fascicolo del dipendente, provvedimenti disciplinari, indagini interne, ecc.), il livello di classificazione attribuito ad un'informazione deve essere indicato con l'apposizione di una etichetta ben visibile.

Esulano dall'obbligo di etichettatura i documenti destinati agli interessati o persone delegate (ad esempio referti medici, prescrizioni, ecc.) da individuare in una apposita tabella come riportato nell'Allegato 2 – Etichettatura.

Inoltre, nel caso di documento cartaceo o informatico il livello di classificazione deve essere riportato su ogni pagina in un opportuno campo nell'intestazione o nel piè di pagina.

In particolare, l'etichetta riportante il livello di classificazione deve essere inserita:

- nel caso di un documento (cartaceo o informatico), sulla prima pagina o su una seconda pagina dedicata, in alto o in basso.
- nel caso di supporti di memorizzazione, con l'apposizione sul supporto della menzione corrispondente al livello di classificazione assegnato all'informazione che presenta il grado di criticità più elevato.

Per le banche dati, elaborazione e aggiornamento da parte del Responsabile della classificazione di un'apposita lista recante l'indicazione dei nomi delle banche dati e della menzione del livello di classificazione attribuito.

In caso di classificazione temporanea, il documento o il supporto devono contenere inoltre l'indicazione della data o dell'evento oltre la quale essa può considerarsi riclassificata o declassificata.

In caso di riclassificazione, devono essere apposte le etichette corrispondenti al nuovo regime applicato.

3.3.1 Etichette da apporre ai documenti

Le etichette da utilizzare per la classificazione della documentazione cartacea o elettronica dovranno riportare almeno le seguenti informazioni:

Documento ad USO INTERNO

Le informazioni contenute nel presente documento possono essere acquisite ed utilizzate dal personale della Struttura Sanitaria con ordinaria diligenza per esclusive finalità lavorative, consapevole che queste costituiscono un bene da proteggere. È quindi vietato qualsiasi utilizzo delle stesse per finalità personali.

I documenti "ad uso interno" possono circolare liberamente nell'ambito della Struttura Sanitaria ma non sono destinati alla diffusione.

L'eventuale divulgazione esterna può risultare inopportuna rispetto ai diritti e alle libertà dell'interessato. Pertanto, a tal fine è necessario richiedere un'autorizzazione al responsabile della classificazione.

Documento CONFIDENZIALE

Le informazioni contenute nel presente documento possono essere acquisite ed utilizzate solo dal personale della Struttura Sanitaria espressamente autorizzato e per esclusive finalità lavorative, consapevole che queste costituiscono un bene da proteggere. È quindi vietato qualsiasi utilizzo delle stesse per finalità personali.

I documenti "confidenziali" non possono circolare liberamente nell'ambito della Struttura Sanitaria né essere messi a disposizione di terze parti a meno di una preventiva e formale autorizzazione della Struttura Sanitaria e della stipula di specifici accordi di riservatezza.

Poiché l'eventuale divulgazione, interna o esterna, a personale non autorizzato può danneggiare i diritti e le libertà dell'interessato, è indispensabile adottare ogni precauzione necessaria ad impedire la rivelazione di tali informazioni a soggetti non autorizzati ed a garantire il trattamento delle stesse conformemente a quanto previsto dalle direttive della Struttura Sanitaria in materia di privacy.

In caso di divulgazione esterna deve essere sempre richiesta un'autorizzazione al responsabile della classificazione.

Lista di distribuzione

Nominativo……. Unità organizzativa…….

Documento STRETTAMENTE CONFIDENZIALE

Le informazioni contenute nel presente documento possono essere acquisite ed utilizzate solo dal personale della Struttura Sanitaria espressamente incaricato ed autorizzato e per esclusive finalità lavorative, consapevole che queste costituiscono un bene da proteggere. È quindi vietato qualsiasi utilizzo delle stesse per finalità personali.

I documenti "strettamente confidenziali" non possono circolare liberamente nell'ambito della Struttura Sanitaria in quanto vincolati da direttive interne, normative nazionali e internazionali, né essere messi a disposizione di terze parti a meno di una preventiva e formale autorizzazione della Struttura Sanitaria e della stipula di specifici accordi di riservatezza.

Poiché l'eventuale divulgazione, interna o esterna, a personale non autorizzato può ledere gravemente i diritti e le libertà dell'interessato, è indispensabile adottare ogni precauzione necessaria ad impedire la rivelazione di tali informazioni a soggetti non autorizzati ed a garantire il trattamento delle stesse conformemente a quanto previsto dalle direttive della Struttura Sanitaria in materia di privacy.

In caso di divulgazione esterna deve essere sempre richiesta un'autorizzazione al responsabile della classificazione.

Lista di distribuzione

Nominativo……. Unità organizzativa…….

3.3.2 Etichette da apporre ai supporti di memorizzazione

Le etichette da utilizzare per la classificazione dei supporti di memorizzazione dovranno riportare almeno le seguenti informazioni:

- Livello di classificazione delle informazioni contenute;
- Eventuale lista di distribuzione.

3.4 Accesso alle informazioni

L'accesso alle informazioni personali deve essere regolamentato in base al principio del "need to know" e del "need to do", ossia limitato a quelle strettamente necessarie allo svolgimento delle mansioni assegnate in funzione delle specifiche esigenze operative.

In particolare, per le informazioni classificate ad uso *confidenziale o strettamente confidenziale*:

- l'accesso ai documenti (cartacei o informatici) e ai supporti è limitato alla sola lista di distribuzione dei destinatari, menzionata nella preclassificazione o nell'etichetta laddove presente;
- l'accesso alle informazioni residenti nelle banche dati è regolamento mediante profili di autorizzazione che tengono conto del relativo livello di classificazione attribuito.

Indipendentemente dal livello di classificazione l'autorizzazione per l'accesso alla documentazione cartacea ed elettronica da parte di soggetti terzi (ad es. fornitori e consulenti) deve essere regolamentata da un formale documento finalizzato all'impegno alla non divulgazione ed al non utilizzo al di fuori degli ambiti stabiliti delle informazioni trattate (Non Disclosure Agreement).

3.5 Elaborazione delle informazioni

Le informazioni destinate al livello di classificazione *confidenziale e strettamente confidenziale* devono essere elaborate in luoghi e con strumentazioni atte a garantirne un'adeguata protezione (ad es. ubicazione in sale CED dedicate o Postazione di Lavoro site in stanze munite di porte con serratura, elaborazione delle informazioni su architetture di rete logico/fisiche sicure come VLAN dedicate controllate da uno o più livelli di firewall).

3.5.1 Accounting (Tracciamento)

L'accesso da parte degli utenti alle informazioni personali residenti nelle banche dati informatiche deve essere tracciato.

Tutte le modifiche ai documenti (cartacei o informatici) devono essere tracciate riportando l'indicazione delle modifiche e l'autore delle stesse all'interno di una lista di controllo.

L'utilizzo da parte degli utenti delle informazioni personali ad uso *strettamente confidenziale* residenti nelle banche dati informatiche deve essere tracciato, registrato e conservato ai fini della gestione della sicurezza e del non ripudio da parte dei soggetti coinvolti.

Il tracciamento deve garantire:

1. l'attendibilità, l'integrità e l'immodificabilità delle evidenze informatiche raccolte;
2. la riservatezza degli archivi;
3. la fruibilità delle informazioni raccolte ai soli soggetti autorizzati.

Il sistema e le modalità di tracciamento devono soddisfare i requisiti dettagliati nella “Politica per la gestione e la conservazione dei log”.

3.6 Duplicazioni delle informazioni

Le informazioni personali classificate *confidenziali o strettamente confidenziali* possono essere duplicate in numero limitato e ristretto alle esigenze della Struttura Sanitaria. L'eventuale riproduzione deve sempre avvenire in condizioni tali da garantirne la protezione.

La riproduzione integrale o parziale di un'informazione classificata *strettamente confidenziale* è effettuata solo previa autorizzazione scritta del competente Responsabile della classificazione.

3.7 Circolazione delle informazioni

Quando le informazioni classificate *confidenziali o strettamente confidenziali* devono circolare all'interno o all’esterno della Struttura Sanitaria, è necessario adottare idonee precauzioni per assicurarne la protezione.

In particolare, devono essere garantiti gli obblighi di riservatezza imposti dalle normative applicabili al fine di non recare alcun danno all’interessato.

3.7.1 Trasmissione delle informazioni

Nei paragrafi successivi vengono descritte le modalità di trasmissione delle informazioni in funzione del livello di classificazione.

3.7.1.1 Informazioni classificate: Uso interno

Per la trasmissione di informazioni classificate *Uso interno* si applicano le seguenti procedure:

Trasmissione interna

- Consentita senza nessuna restrizione.

Trasmissione esterna

- Autorizzazione del responsabile della classificazione dell’informazione per la circolazione esterna;
- Invio per posta semplice con l’indicazione del nominativo del destinatario;
- Invio tramite posta elettronica della Struttura Sanitaria.

3.7.1.2 Informazioni classificate: Confidenziali

Per la trasmissione di informazioni classificate confidenziali si applicano le seguenti procedure:

Trasmissione interna

- Consegna "brevi manu" o in busta semplice recante la menzione CONFIDENZIALE e l'indicazione del nominativo del destinatario della spedizione oppure trasmissione via fax con presidio fisico alla ricezione;
- Posta elettronica della Struttura Sanitaria, purché il destinatario sia nominativamente specificato e riceva personalmente l'informazione.

Trasmissione esterna

- Autorizzazione del responsabile della classificazione dell'informazione per la circolazione esterna;
- Raccomandata con ricevuta di ritorno in busta semplice recante la menzione CONFIDENZIALE e l'indicazione del nominativo del destinatario della spedizione;
- Invio tramite posta elettronica della Struttura Sanitaria con ricevuta di avvenuta consegna e conferma di lettura, purché il destinatario sia nominativamente specificato e riceva personalmente l'informazione. L'oggetto del messaggio deve anche recare la menzione CONFIDENZIALE;
- Utilizzo di canali di comunicazione sicura come VPN, linee dedicate o soluzioni equivalenti, in accordo con quanto definito dalle politiche della Struttura Sanitaria;
- Nel caso di trasmissione tra elaboratori, utilizzo di canali di comunicazione sicura come VPN, linee dedicate o soluzioni equivalenti, in accordo con quanto definito dalle politiche della Struttura Sanitaria.

3.7.1.3 Informazioni classificate: Strettamente confidenziali

Per la trasmissione di informazioni classificate strettamente confidenziali si applicano le seguenti procedure.

Trasmissione interna

- Consegna "brevi manu" esclusivamente dal personale della Struttura Sanitaria autorizzato direttamente al destinatario;
- Raccomandata di servizio recante il nominativo del destinatario. Il documento è posto in doppia busta e la busta esterna non reca alcun segno distintivo, mentre la busta interna sigillata reca la menzione STRETTAMENTE CONFIDENZIALE;

- Trasmissione via fax con l'adozione di meccanismi tali da garantirne la riservatezza (ad es. cifratura della trasmissione) e presidio fisico alla ricezione;
- Invio tramite posta elettronica della Struttura Sanitaria, solo se consentito dalle policy aziendali, di un messaggio cifrato recante il nome del destinatario ovvero invio di informazioni pseudonimizzate dal mittente prima dell'invio;
- Nel caso di trasmissione tra elaboratori, utilizzo di canali sicuri, in accordo con quanto definito dalle politiche della Struttura Sanitaria.

Trasmissione esterna

- Autorizzazione del responsabile della classificazione dell'informazione per la circolazione esterna;
- Invio con plico raccomandato con ricevuta di ritorno o invio tramite corriere privato. Il destinatario della spedizione deve sempre essere designato nominativamente. Il documento è posto in doppia busta e la busta esterna non reca alcun segno distintivo, mentre la busta interna sigillata reca la menzione STRETTAMENTE CONFIDENZIALE;
- Invio attraverso posta elettronica della Struttura Sanitaria, solo se consentito dalle policy aziendali, che deve avvenire in modo tale da garantire la riservatezza di quanto trasmesso (ad es. tramite messaggio cifrato recante il nome del destinatario, utilizzo di PEC con allegato cifrato);
- Utilizzo di canali di comunicazione sicura come VPN, linee dedicate o soluzioni equivalenti, in accordo con quanto definito dalle politiche della Struttura Sanitaria;
- Nel caso di trasmissione tra elaboratori, utilizzo di soluzioni crittografiche per la cifratura delle informazioni oltre a canali di comunicazione sicura come VPN, linee dedicate o soluzioni equivalenti, in accordo con quanto definito dalle politiche della Struttura Sanitaria.

3.8 Conservazione delle informazioni

Le informazioni personali non possono essere lasciate in evidenza nei luoghi di lavoro in particolare negli ambienti accessibili al pubblico. Queste informazioni non devono essere lasciate incustodite.

Le informazioni classificate ad uso *confidenziale*, contenute in documenti cartacei o in supporti di memorizzazione, devono essere conservate in mobili chiusi a chiave (ad es. armadi, cassettiere, ecc.), mentre le informazioni classificate ad uso *strettamente confidenziale* devono essere

conservate in armadi la cui resistenza ed il cui dispositivo di chiusura sono considerati sicuri e affidabili.

Le informazioni classificate ad uso *strettamente confidenziale*, contenute in documenti elettronici o base dati devono essere conservate centralmente e sottoposte a backup secondo quanto previsto dalle politiche della Struttura Sanitaria.
Le informazioni classificate ad uso *confidenziale* contenute in documenti elettronici o base dati possono altresì risiedere in locale sulle postazioni lavorative. In questo caso il back-up deve essere effettuato localmente nell'ambito dell'ufficio su idonei supporti di memorizzazione (ad es. hard disk esterni, CD, DVD, Token USB, ecc.), opportunamente etichettati, in grado di assicurare l'inalterabilità nel tempo e la disponibilità dell'informazione, in accordo con le politiche della Struttura Sanitaria.

La riservatezza delle informazioni classificate ad uso *strettamente confidenziale*, memorizzate su supporti rimovibili deve essere garantita attraverso opportuni algoritmi di cifratura e compressione, come definito nell'apposita Policy [12]. Per quanto riguarda le banche dati, tale valutazione deve essere effettuata a seguito delle valutazioni di analisi dei rischi privacy (DPIA). Per quanto concerne le informazioni ad uso *confidenziale*, tale indicazione seppur opzionale è raccomandata in quanto è in grado di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, delle informazioni stesse o di accesso non autorizzato o di trattamento non consentito.
Il Responsabile della Classificazione valuterà autonomamente l'applicazione di tale misura idonea.

I supporti rimovibili contenenti informazioni classificate ad uso *confidenziale* e *strettamente confidenziale* possono essere riutilizzati solo se le informazioni in essi precedentemente contenute non siano intelligibili e tecnicamente in alcun modo ricostruibili, come definito nell'apposita Policy [11].

3.9 Cancellazione e distruzione delle informazioni

Le informazioni classificate devono essere opportunamente cancellate o distrutte nei casi di seguito riportati:

- non siano più utili al raggiungimento delle finalità lavorative;

- siano relative a trattamenti non più necessari, secondo correttezza;
- risultino non pertinenti, incomplete ed eccedenti rispetto alle finalità per le quali sono state raccolte o successivamente trattate;
- risultino inesatte o non aggiornate;
- gli scopi per i quali sono state raccolte e trattate non siano più determinati, espliciti e legittimi;
- risultino scaduti i termini legittimi di conservazione siano essi determinati da norme di legge generali e/o di settore o dalle finalità per le quali i dati sono stati raccolti.

La cancellazione o distruzione delle informazioni deve avvenire, in accordo con quanto previsto dalla Politica per la Cancellazione Sicura e lo Smaltimento dei Supporti Elettronici della Struttura Sanitaria [11], con modalità che tengano conto della classificazione delle informazioni stesse e consentano l'eliminazione irreversibile dei dati contenuti in un supporto elettronico in modo che essi non siano più accessibili a terzi o risultino comunque inintelligibili e impedendo così il recupero degli stessi (modalità di cancellazione sicura). A titolo esemplificativo, ma non esaustivo:

- la distruzione della documentazione cartacea classificata deve essere effettuata con appositi distruggi documenti o mediante altre procedure di distruzione autorizzate dalla Struttura Sanitaria;
- la cancellazione della documentazione elettronica deve essere effettuata mediante procedure atte a garantire la non recuperabilità delle informazioni;
- i supporti di memorizzazione dismessi contenenti informazioni classificate confidenziali o strettamente confidenziali possono essere smaltiti solo previa eliminazione permanente delle informazioni memorizzate.

3.10 Istruzioni al personale

Devono essere impartite specifiche istruzioni al fine di rendere edotto il personale della Struttura Sanitaria:

- sulle presenti linee guida di classificazione delle informazioni;
- sulle modalità operative di gestione delle informazioni classificate;
- sulle responsabilità derivanti dalla mancata ottemperanza delle istruzioni impartite;
- sulle misure di protezione da attuare durante lo svolgimento delle mansioni lavorative.

3.11 Protezione delle informazioni

Le informazioni personali devono essere adeguatamente protette. A tal fine, chiunque le acquisisca o le utilizzi deve adottare opportune misure tecnologiche, organizzative e procedurali di sicurezza e provvedere affinché esse circolino o siano divulgate solo ove strettamente necessario per le esigenze lavorative.

3.11.1 Requisiti di sicurezza

Si riportano di seguito la sintesi dei requisiti di sicurezza di carattere generale associati a ciascun livello di classificazione. Tali requisiti devono essere implementati, al fine di assicurare un livello minimo di sicurezza delle informazioni in base alla relativa classificazione.

3.11.1.1 Livello di classificazione: Uso Interno

Livello di classificazione: Uso interno	
Azione	**Requisito**
Etichettatura	Per i documenti (cartacei o informatici), inserimento: ▪ dell'etichetta sulla prima pagina o su una seconda pagina, in alto o in basso; ▪ del grado di classificazione su ogni pagina in un opportuno campo nell'intestazione o nel piè di pagina. Per i supporti di memorizzazione, apposizione sul supporto della menzione corrispondente. Per le banche dati, elaborazione da parte del Responsabile della classificazione di un'apposita lista recante l'indicazione dei nomi delle banche dati e della menzione del livello di classificazione attribuito. Aggiornamento della lista.
Accesso alle informazioni	Nessuna restrizione per l'accesso alle informazioni da parte del personale interno. Autorizzazione per l'accesso da parte di soggetti terzi solo con impegno alla non divulgazione ed al non utilizzo al di fuori degli ambiti stabiliti (NDA). L'accesso alle informazioni residenti nelle banche dati è regolamento mediante profili di autorizzazione che tengono conto del relativo livello di classificazione attribuito.
Assegnazione diritti di accesso	Responsabile della classificazione.
Elaborazione delle informazioni	Nessuna restrizione per l'elaborazione delle informazioni da parte del personale interno e di soggetti esterni preventivamente autorizzati.
Accounting (Tracciamento)	L'accesso da parte degli utenti alle informazioni residenti nelle banche dati deve essere tracciato.
Duplicazione delle informazioni	Nessuna restrizione.
Trasmissione interna	Nessuna restrizione.
Trasmissione esterna	Autorizzazione del responsabile della classificazione per la circolazione esterna. Invio per posta semplice recante l'indicazione del nominativo del

Livello di classificazione: Uso interno	
Azione	**Requisito**
	destinatario. Invio per posta elettronica della Struttura Sanitaria.
Conservazione delle informazioni	Le informazioni personali non devono essere lasciate in evidenza/incustodite, soprattutto in ambienti accessibili al pubblico.
Distruzione	Per la documentazione cartacea, utilizzo di appositi distruggi documenti o di altre procedure di distruzione autorizzate della Struttura Sanitaria. Per la documentazione elettronica cancellazione mediante procedure atte a garantire la non recuperabilità delle informazioni.

Tabella 3 – Requisiti di sicurezza "Uso interno"

3.11.1.2 Livello di classificazione: Confidenziale

Livello di classificazione: Confidenziale	
Azione	**Requisito**
Etichettatura	Per i documenti (cartacei o informatici), inserimento: ▪ dell'etichetta sulla prima pagina o su una seconda pagina, in alto o in basso; ▪ del grado di classificazione su ogni pagina in un opportuno campo nell'intestazione o nel piè di pagina; ▪ della lista di distribuzione dei destinatari. Per i supporti di memorizzazione, apposizione sul supporto della menzione corrispondente. Elaborazione di una lista di distribuzione dei destinatari. Per le banche dati, elaborazione da parte del Responsabile della classificazione di un'apposita lista recante l'indicazione dei nomi delle banche dati e della menzione del livello di classificazione attribuito. Aggiornamento della lista.
Accesso alle informazioni	Autorizzazione per l'accesso alla documentazione cartacea ed elettronica limitati alla lista di distribuzione. Autorizzazione per l'accesso da parte di soggetti terzi solo con impegno alla non divulgazione ed al non utilizzo al di fuori degli ambiti stabiliti (NDA). L'accesso alle informazioni residenti nelle banche dati è regolamento mediante profili di autorizzazione che tengono conto del relativo livello di classificazione attribuito.
Assegnazione diritti di accesso	Responsabile della classificazione.
Elaborazione delle informazioni	Elaborazione delle informazioni elettroniche su architetture di rete logico/fisiche sicure come VLAN dedicate controllate da uno o più livelli di firewall. Postazioni di lavoro site in stanze munite di porte con serratura. Ubicazione delle banche dati in sale CED dedicate.
Accounting (Tracciamento)	L'accesso da parte degli utenti alle informazioni residenti nelle banche dati deve essere tracciato. Tutte le modifiche ai documenti (cartacei o elettronici) devono essere tracciate riportando la modifica apportata e l'autore della

Livello di classificazione: Confidenziale	
Azione	**Requisito**
	stessa all'interno di una lista di controllo.
Duplicazione delle informazioni	Per la documentazione cartacea ed elettronica, duplicazione in numero limitato e ristretto alle esigenze della Struttura Sanitaria secondo procedure atte a garantirne la protezione.
Circolazione delle informazioni	Autorizzazione del responsabile della classificazione. Stipula di accordi di riservatezza con le terze parti.
Trasmissione interna	Consegna "brevi manu" o in busta semplice recante la menzione CONFIDENZIALE ed il nome del destinatario oppure trasmissione via fax con presidio fisico alla ricezione. Posta elettronica della Struttura Sanitaria, purché il destinatario sia nominativamente indicato e riceva personalmente l'informazione.
Trasmissione esterna	Autorizzazione del responsabile della classificazione per la circolazione esterna. Raccomandata con ricevuta di ritorno in busta semplice recante la menzione CONFIDENZIALE e l'indicazione del nominativo del destinatario. Posta elettronica della Struttura Sanitaria con ricevuta di avvenuta consegna e conferma di lettura, purché il destinatario sia nominativamente indicato e riceva personalmente l'informazione. Nel caso di trasmissione tra elaboratori, utilizzo di canali di comunicazione sicura come VPN, linee dedicate o soluzioni equivalenti.
Conservazione delle informazioni	Per la documentazione cartacea o supporti di memorizzazione, conservazione in mobili chiusi a chiave. Per la documentazione elettronica comprese le base dati, possibilità di conservazione su supporti fissi (anche in locale sui PC), in grado di assicurare l'inalterabilità nel tempo e la disponibilità dell'informazione, in accordo con le politiche della Struttura Sanitaria. Cifratura delle informazioni come requisito opzionale in funzione di quanto indicato dal Responsabile della classificazione
Distruzione	Per la documentazione cartacea, utilizzo di appositi distruggi documenti o di altre procedure di distruzione autorizzate della Struttura Sanitaria. Per la documentazione elettronica cancellazione mediante

Livello di classificazione: Confidenziale	
Azione	**Requisito**
	procedure atte a garantire la non recuperabilità delle informazioni. Per i supporti di memorizzazione dismessi, smaltimento solo previa eliminazione permanente delle informazioni memorizzate.

Tabella 4 – Requisiti di sicurezza "Confidenziale"

3.11.1.3 Livello di classificazione: Strettamente confidenziale

Livello di classificazione: Strettamente confidenziale	
Azione	**Requisito**
Etichettatura	Per i documenti (cartacei o informatici), inserimento: ▪ dell'etichetta sulla prima pagina o su una seconda pagina, in alto o in basso; ▪ del grado di classificazione su ogni pagina in un opportuno campo nell'intestazione o nel piè di pagina; ▪ della lista di distribuzione dei destinatari. Per i supporti di memorizzazione, apposizione sul supporto della menzione corrispondente. Elaborazione di una lista di distribuzione dei destinatari. Per le banche dati, elaborazione da parte del Responsabile della classificazione di un'apposita lista recante l'indicazione dei nomi delle banche dati e della menzione del livello di classificazione attribuito. Aggiornamento della lista.
Accesso alle informazioni	Autorizzazione per l'accesso alla documentazione cartacea ed elettronica limitati alla lista di distribuzione. Autorizzazione per l'accesso da parte di soggetti terzi solo con impegno alla non divulgazione ed al non utilizzo al di fuori degli ambiti stabiliti (NDA). L'accesso alle informazioni residenti nelle banche dati è regolamento mediante profili di autorizzazione che tengono conto del relativo livello di classificazione attribuito.
Assegnazione diritti di accesso	Responsabile della classificazione.

Livello di classificazione: Strettamente confidenziale	
Azione	**Requisito**
Elaborazione delle informazioni	Tutte le modifiche alle informazioni devono essere tracciate. Nei documenti (cartacei o elettronici), l'indicazione delle modifiche deve essere inserita all'interno di una lista di controllo. Elaborazione delle informazioni su architetture di rete logico/fisiche sicure come VLAN dedicate controllate da uno o più livelli di firewall. Postazioni di lavoro site in stanze munite di porte con serratura. Ubicazione delle banche dati in sale CED dedicate.
Accounting (Tracciamento)	L'accesso e l'utilizzo da parte degli utenti delle informazioni residenti nelle banche dati deve essere tracciato. Tutte le modifiche ai documenti (cartacei o elettronici) devono essere tracciate riportando la modifica apportata e l'autore della stessa all'interno di una lista di controllo.
Duplicazione delle informazioni	Per la documentazione cartacea ed elettronica, duplicazione in numero limitato e ristretto alle esigenze della Struttura Sanitaria secondo procedure atte a garantirne la protezione. La riproduzione integrale e parziale di un'informazione è effettuata solo previa autorizzazione scritta del Responsabile della classificazione.
Circolazione delle informazioni	Autorizzazione del Responsabile della classificazione. Stipula di accordi di riservatezza con le terze parti.
Trasmissione interna	Consegna "brevi manu" direttamente al destinatario effettuata esclusivamente dal personale della Struttura Sanitaria autorizzato. Raccomandata di servizio recante il nominativo del destinatario, con documento è posto in doppia busta e la busta esterna non reca alcun segno distintivo, mentre la busta interna sigillata reca la menzione STRETTAMENTE CONFIDENZIALE. Invio tramite fax con adozione di meccanismi tali da garantirne la riservatezza (ad es. cifratura della trasmissione) e presidio fisico alla ricezione. Invio tramite posta elettronica della Struttura Sanitaria, solo se consentito dalle policy aziendali, di un messaggio cifrato recante il nome del destinatario, ovvero invio di informazioni pseudonimizzate dal mittente prima dell'invio. Per le trasmissioni tra elaboratori, utilizzo di canali sicuri.
Trasmissione esterna	Autorizzazione del responsabile della classificazione per la

Livello di classificazione: Strettamente confidenziale	
Azione	**Requisito**
	circolazione esterna. Invio con plico raccomandato con ricevuta di ritorno o invio tramite corriere privato. Il documento è posto in doppia busta e la busta esterna non reca alcun segno distintivo, mentre la busta interna sigillata reca la menzione STRETTAMENTE CONFIDENZIALE. Il destinatario della spedizione deve essere nominativamente indicato. Invio tramite posta elettronica della Struttura Sanitaria, solo se consentito dalle policy aziendali, in modo tale da garantire la riservatezza di quanto trasmesso. Utilizzo di canali di comunicazione sicura come VPN, linee dedicate o soluzioni equivalenti. Per le trasmissioni tra elaboratori, utilizzo di soluzioni crittografiche per la cifratura delle informazioni associate a VPN o linee dedicate o soluzioni equivalenti.
Conservazione delle informazioni	Per la documentazione cartacea o supporti rimovibili, conservazione in armadi la cui resistenza e il cui dispositivo di chiusura sono considerati sicuri e affidabili (ad es. lucchetto, combinazione elettronica, ecc.). Per la documentazione elettronica comprese le base dati, conservazione centralizzata e adozione di misure di protezione in linea con le valutazioni delle DPIA. Per la memorizzazione su supporti rimovibili adozione di cifratura e compressione secondo le politiche della Struttura Sanitaria.
Distruzione	Per la documentazione cartacea, utilizzo di appositi distruggi documenti o di altre procedure di distruzione autorizzate della Struttura Sanitaria. Per la documentazione elettronica cancellazione mediante procedure atte a garantire la non recuperabilità delle informazioni. Per i supporti di memorizzazione dismessi, smaltimento solo previa eliminazione permanente delle informazioni memorizzate.

Tabella 5 – Requisiti di sicurezza “Strettamente confidenziale”

4 Classificazione dei Trattamenti

Tutti i trattamenti effettuati dalla Struttura Sanitaria, afferenti alle seguenti informazioni devono essere oggetto di classificazione:

- dati personali (ai sensi dell'art. 4 del GDPR [1]);
- categorie particolari di dati personali (ai sensi dell'art. 9 del GDPR [1]);
- dati personali relativi a condanne penali e reati (ai sensi dell'art. 10 del GDPR [1]).

La classificazione del trattamento, eseguita attraverso una valutazione del livello di classificazione delle informazioni e della tipologia del trattamento, deve essere effettuata dalla persona responsabile del processo, del progetto o dell'unità organizzativa a cui afferisce il trattamento stesso, nel momento in cui viene inserito nel registro dei trattamenti ovvero ogni qualvolta si verifica una variazione nella tipologia di informazioni trattate o del trattamento.

Criticità del trattamento	Descrizione
Bassa	Trattamenti per i quali vengono utilizzati dati personali classificati ad uso interno.
Media	Trattamenti per i quali vengono utilizzati dati personali classificati confidenziali.
Alta	Trattamenti per i quali vengono utilizzati dati personali strettamente confidenziali e/o che ricadono nelle tipologie di cui al provvedimento del Garante [13], di seguito sintetizzate: 1. Trattamenti valutativi o di scoring su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive; 2. Trattamenti automatizzati finalizzati ad assumere decisioni che producono "effetti giuridici" oppure che incidono "in modo analogo significativamente" sull'interessato; 3. Trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti; 4. Trattamenti su larga scala di dati aventi carattere estremamente personale; 5. Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei

Criticità del trattamento	Descrizione
	dipendenti; 6. Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo); 7. Trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo; 8. Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche; 9. Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni; 10. Trattamenti di categorie particolari di dati personali oppure di dati personali relativi a condanne penali e a reati interconnessi con altri dati personali raccolti per finalità diverse; 11. Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento; 12. Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.

5 Allegato 1 – Preclassificazione delle informazioni

Al fine di agevolare la classificazione dei dati personali, è opportuno effettuare una preclassificazione delle informazioni normalmente trattate dalla Struttura Sanitaria, individuando per ciascuna tipologia il relativo livello di classificazione e la lista di distribuzione, secondo la tabella riportata di seguito.

Nella lista di distribuzione può essere inserito un singolo destinatario, una tipologia oppure una struttura organizzativa.

Nella tabella sottostate sono riportati alcuni esempi di possibili informazioni con il relativo livello di classificazione.

Informazione	Livello classificazione	Lista di distribuzione
Cartella clinica	Strettamente confidenziale	
Referto	Strettamente confidenziale	
Prescrizione medica	Strettamente confidenziale	
Data base anagrafica assistiti	Confidenziale	
Piano turni del personale	Confidenziale	
Rubrica telefonica del personale	Uso interno	
Ordini di servizio	Uso interno	

6 Allegato 2 – Etichettatura

Al fine di agevolare l'individuazione della necessità di apporre l'etichetta sui documenti e/o sui supporti di memorizzazione viene fornita una tabella di riferimento nella quale inserire le tipologie di documenti o i supporti di memorizzazione che non sono soggetti ad obbligo di etichettatura.

Tipo documento/supporto di memorizzazione che non richiede etichettatura