Policy sulla conservazione dei Dati Personali

INFORMAZIONI DOCUMENTO:

Titolo	Policy sulla conservazione dei Dati Personali		
Data di emissione	25 maggio 2018	**Versione**	1.0

SOMMARIO

I. INTRODUZIONE

A. SCOPO

La presente "Policy sulla conservazione dei Dati Personali" riporta i criteri utilizzati dalla società Ospedale San Raffaele S.r.l. (infra "**Società**") per la conservazione dei Dati Personali.
Salvo diversamente previsto all'interno di questo documento, tutti i termini riportati con lettera iniziale maiuscola si riferiscono alle definizioni riportate nel GDPR e riportate per comodità nella sezione "Glossario e Acronimi".

B. NORMATIVA DI RIFERIMENTO

Articolo 5
Principi applicabili al trattamento di dati personali
1. I dati personali sono:
a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);
c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);
f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).
2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»).

Articolo 13
Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato
1. In caso di raccolta presso l'interessato di dati che lo riguardano, il titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:
a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;

b) i dati di contatto del responsabile della protezione dei dati, ove applicabile;
c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
d) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.
2. In aggiunta alle informazioni di cui al paragrafo 1, nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente:
a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
b) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
c) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
d) il diritto di proporre reclamo a un'autorità di controllo;
e) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
f) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.
3. Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente di cui al paragrafo 2.
4. I paragrafi 1, 2 e 3 non si applicano se e nella misura in cui l'interessato dispone già delle informazioni.

C. DOCUMENTI DI RIFERIMENTO

1. Regolamento Generale sulla Protezione dei dati personali (UE) 2016/679
2. Procedura sull'esercizio dei diritti dell'Interessato
3. Linee guida sulle Persone Autorizzate al Trattamento dei Dati Personali
4. Registro dei Trattamenti ex art. 30 GDPR
5. Privacy Policies

6. Policy sulla conservazione dei Dati Personali
7. Linee guida sul data protection by design e by default
8. Linee guida sulla formazione
9. Policy Strumenti IT
10. Manuale di gestione della Documentazione Sanitaria e Socio Sanitaria", (successivamente parzialmente modificato dalla d.g.r. n. X/325 del 2013)
11. Decreto N. 15229 del 01/12/2017 della Regione Lombardia approvazione della "versione 04" del "Titolario e massimario del sistema sociosanitario lombardo, già sistema sanitario e sociosanitario di regione Lombardia".

D. GLOSSARIO E ACRONIMI

Archivio: qualsiasi insieme strutturato di Dati Personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

Aree Sensibili: sono quei luoghi fisici o della Rete Aziendale in cui vengono Trattati Dati Particolari e/o Dati Giudiziari relativi a persone fisiche; e/o luoghi in cui vengono gestiti e consultati documenti riservati a cui è assolutamente vietato accedere se non per motivi di servizio;

Autorità di Controllo: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 GDPR;

Consenso dell'Interessato o **Consenso**: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'Interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i Dati Personali che lo riguardano siano oggetto di Trattamento;

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 Comuni: sono tutti i Dati Personali che non appartengono alle categorie dei Dati Particolari e Dati Giudiziari;

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 Giudiziari: Dati Personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza;

Dati Particolari: Dati Personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare 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 relativi alla Salute: i Dati Personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

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

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

Device Fissi: si intendono gli strumenti informatici non facilmente removibili dal perimetro aziendale quali personal computer, server locali, stampanti affidati alle Persone Autorizzate per uso professionale;

Device Mobili: in generale si intendono quegli strumenti informatici che per loro natura sono facilmente asportabili dal perimetro aziendale quali chiavette USB, SD cards, hard disk esterni, tablet e smartphone utilizzati dalla Persone Autorizzate per uso professionale;

DPO o **Data Protection Officer**: è una persona fisica, nominata obbligatoriamente nei casi di cui all'art. 37.1 GDPR dal Titolare o dal Responsabile del Trattamento e deve possedere una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati per assisterli nel rispetto a livello interno del GDPR;

GDPR o **Regolamento:** Regolamento Generale sulla Protezione dei dati personali (UE) 2016/679.

Gruppo Imprenditoriale: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

Incaricato/i o Persona/e Autorizzata/e: si tratta dei Collaboratori autorizzati al Trattamento dei Dati Personali sotto la diretta autorità del Titolare e/o del Responsabile ex artt. 4(10) e 29 del GDPR. Stante la definizione fornita dal Gruppo di Lavoro Articolo 29 dell'Opinione 2/2017 questa definizione ricomprende:

dipendenti ed ex dipendenti, dirigenti, sindaci, collaboratori e lavoratori a partita IVA, lavoratori a chiamata, part-time, *job-sharing*, contratti a termine, stage, senza distinzione di ruolo, funzione e/o livello, nonché consulenti e fornitori della Società e, più in generale, tutti coloro che utilizzino od abbiano utilizzato Strumenti Aziendali o Strumenti Personali, operino sulla Rete Aziendale ovvero siano a conoscenza di informazioni aziendali rilevanti quali, a titolo esemplificativo e non esaustivo: (a) i Dati Personali di clienti, dipendenti e fornitori, compresi gli indirizzi di posta elettronica; (b) tutte le informazioni aventi ad oggetto informazioni confidenziali di natura commerciale, finanziaria o di strategia di business; nonché (c) i dati e le informazioni relative ai processi aziendali, inclusa la realizzazione di marchi, brevetti e diritti di proprietà industriale, la cui tutela prescinde dagli effetti pregiudizievoli che potrebbe comportare la diffusione delle medesime.

Limitazione Di Trattamento: il contrassegno dei Dati Personali conservati con l'obiettivo di limitarne il Trattamento in futuro;

Processo Decisionale Automatizzato: decisione basata unicamente sul Trattamento automatizzato, compresa la Profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona;

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

Pseudonimizzazione: il Trattamento dei Dati Personali in modo tale che i Dati Personali non possano più essere attribuiti a un Interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali Dati Personali non siano attribuiti a una persona fisica identificata o identificabile;

Rappresentante: la persona fisica o giuridica stabilita nell'Unione che, designata dal Titolare del trattamento o dal Responsabile del trattamento per iscritto ai sensi dell'articolo 27 GDPR, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del GDPR;

Responsabile del Trattamento o **Responsabile**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta Dati Personali per conto del Titolare del Trattamento; deve presentare garanzie sufficienti di attuare misure tecniche e organizzative adeguate in modo tale che il Trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'Interessato;

Sistema Informativo Aziendale : rappresenta il perimetro digitale della Società contenente Dati Personali e/o informazioni riservate fruibili dalla rete interna (intranet) e/o dalla rete esterna (internet)

Strumenti Aziendali: l'insieme di Device Fissi e Device Mobili concessi in comodato d'uso dalla Società alle Persone Autorizzate al fine di svolgere le proprie mansioni;

Strumenti Personali: i Device di proprietà delle Persone Autorizzate autorizzati ad essere impiegati per uso professionale;

Terzo: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'Interessato, il Titolare del Trattamento, il Responsabile del Trattamento e le Persone Autorizzate al Trattamento dei Dati Personali sotto l'autorità diretta del Titolare o del Responsabile;

Titolare del Trattamento o **Titolare:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del Trattamento di Dati Personali; quando le finalità e i mezzi di tale Trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il Titolare o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

Trattamento o **Trattato/Trattati:** 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;

Trattamento Transfrontaliero: a) Trattamento di Dati Personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un Titolare del Trattamento o Responsabile del Trattamento nell'Unione ove il Titolare o il Responsabile siano stabiliti in più di uno Stato membro; oppure, b) Trattamento di Dati Personali che ha luogo nell'ambito delle attività di un unico stabilimento di un Titolare o Responsabile nell'Unione, ma che incide o probabilmente incide in modo sostanziale su Interessati in più di uno Stato membro;

Violazione Dei Dati Personali ovvero **Data Breach:** è la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai Dati Personali trasmessi, conservati o comunque Trattati.

II. CRITERI SULLA CONSERVAZIONE DEI DATI PERSONALI

Con l'entrata in vigore del GDPR, la Società ha l'obbligo di definire il periodo di conservazione dei Dati Personali oppure, se ciò non è possibile, i criteri utilizzati per determinare tale periodo.
In considerazione del fatto che determinare un criterio astratto è più semplice, oltre che metodologicamente più corretto, per arrivare ad uno specifico periodo di conservazione, la Società elenca i macro-criteri di conservazione identificati.

Progressivamente, la Società procederà, secondo il principio di responsabilizzazione, a definire, ove possibile, i periodi esatti di conservazione.
I criteri e i periodi di conservazione sono costantemente aggiornati nel Registro dei Trattamenti ex art. 30, se previsto, e in ogni caso nelle Privacy Policies.

A. CRITERIO DI NECESSITÀ

Vengono conservati tutti i Dati Personali necessari a raggiungere lo scopo per il quale sono stati raccolti e per il tempo necessario a raggiungere tale scopo (es.: dati conservati in costanza di rapporto contrattuale e per tutta la sua durata).

B. OBBLIGO DI LEGGE

Vengono conservati tutti i Dati Personali che la normativa vigente (es.: fiscale, giuslavoristica) impone di conservare, per il tempo richiesto dalla normativa stessa (es. normativa sulla conservazione dei dati di traffico).

C. OPPORTUNITÀ

Vengono conservati i Dati Personali che la legge dà facoltà di conservare, per il tempo suggerito dalla normativa oppure stabilito dal Titolare. È il caso ad esempio dei dati conservati per finalità di difesa in giudizio da azioni di natura contrattuale o extracontrattuale. Nel primo caso, verranno conservati solo – ed esclusivamente - i Dati Personali necessari, ad esempio, ad avere correttamente erogato il servizio contrattualizzato, per dieci anni dalla cessazione del rapporto contrattuale; nel secondo caso, si conserveranno per cinque anni i dati necessari a difendersi in giudizio da azioni di natura extracontrattuale. Ancora, è il caso dei dati raccolti e trattati per finalità di marketing, riferiti a soggetti con cui non si ha più un rapporto contrattuale, conservati fino alla revoca del Consenso da parte dell'Interessato.

Seguono alcuni esempi di periodi di conservazione già identificati: concreti:

- Dati Personali raccolti e trattati per finalità di marketing riferiti a soggetti con cui la Società non ha più un rapporto contrattuale: questi sono conservati fino alla revoca del Consenso da parte dell'Interessato;
- i dati raccolti e trattati per finalità di Profilazione: in astratto sono conservati fino a revoca del Consenso, salvo ulteriori chiarimenti che l'Autorità di Controllo competente vorrà fornire;

D. MASSIMARIO DI SCARTO

La società, nella definizione della *data retention* della documentazione, a prescindere dal tipo di supporto, cartaceo o digitale, sul quale è prodotta, fa riferimento ai tempi stabiliti nel Massimario di scarto *"Versione 04" del* ***"Titolario e Massimario del Sistema Sociosanitario Lombardo, già Sistema Sanitario e Sociosanitario di Regione Lombardia", Allegato 1, parte integrante del presente atto, che sostituisce integralmente il precedente, approvato con Decreto del D.G. Welfare n. 11466 del***

***17.12.2015* e s.i.m.**; adottato da Regione Lombardia che si applica a tutto il Sistema Socio-sanitario Lombardo e che si intende nella presente procedura integralmente richiamato.

E. DOSSIER SANITARIO ELETTRONICO

La durata della conservazione dei dati relativi agli eventi clinici dei pazienti/interessati, contenuti nel Dossier Sanitario Elettronico è legata al perdurare del consenso ex art. 9.2.a) del GDPR.

I log delle operazioni effettuate nel dossier sanitario elettronico da parte degli incaricati devono essere conservati per 24 mesi dalla registrazione dell'operazione.