SISTEMA GESTIONE PRIVACY PRESIDIO ANNA TORRIGIANI

PREMESSA

Il Presidio Anna Torrigiani, in qualità di Titolare del trattamento, è il soggetto che garantisce che i trattamenti di dati personali effettuati per l'adempimento delle proprie attività istituzionali si svolgano nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali; provvede al trattamento dei dati personali nel rispetto dei principi generali di cui all'art. 5 del Regolamento Europeo sulla protezione dei dati personali, in particolare dei principi di semplificazione, liceità, correttezza e trasparenza. Il contenuto del presente documento è destinato a tutti gli interessati, referenti privacy e responsabili del trattamento nonché a tutti i soggetti autorizzati che effettuano operazioni di trattamento dati personali per conto del Presidio Sanitario allo scopo di garantire e proteggere i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento dei propri dati personali.

Il Management aziendale ha determinato la necessità di adeguare la policy, le procedure e i regolamenti aziendali al fine di garantire la compliance alle indicazioni del Regolamento UE 679/2016 (GDPR) e della normativa nazionale in materia di privacy. A tale scopo, il Direttore Generale, in qualità di Titolare del trattamento, con il supporto del Responsabile delle Protezione dei Dati aziendale, verificata la congruità agli obiettivi aziendali e alle disposizioni legislative nazionali ed europee, ha identificato il percorso organizzativo da attuare. La procedura operativa definisce le azioni che saranno messe in atto dall'azienda per adempiere alla normativa.

Il percorso operativo prevede le seguenti fasi:

A) Definizione di una Strategia aziendale condivisa di trattamento dei dati personali;

B) Mappatura dei trattamenti, dell'organizzazione e delle procedure esistenti,

C) Ridefinizione dei processi e delle metodologie di trattamento

D) Implementazione di un Sistema di Gestione della Protezione dei Dati strutturato, per garantire una gestione efficace ed efficiente dei requisiti normativi in ottica di continuo miglioramento

E) Monitoraggio e Controllo.

DEFINIZIONI

Il dato personale*: qualsiasi informazione riguardante una persona fisica identificata o identificabile.*
Il dato sensibile*: qualsiasi dato personale idoneo a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.*
Il dato relativo alla salute*: qualsiasi dato personale attinente 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.*

Il dato genetico*: qualsiasi dato personale relativo 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.*

Il dato biometrico*: qualsiasi dato personale ottenuto da un trattamento tecnico specifico relativo 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.*

Il 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*

Ambito sanitario*: il contesto organizzativo, funzionale e professionale in cui soggetti specificamente autorizzati svolgono attività finalizzate alla tutela della salute, nelle quali e per le quali è essenziale il trattamento di dati idonei a rivelare lo stato di salute degli interessati.*

Dossier sanitario*: banca dati elettronica comprendente dati e documenti sanitari in possesso di uno specifico Organismo, relativi ad uno o più percorsi di cura effettuati presso di esso da un certo assistito. Banca dati dinamica ed accessibile nel suo complesso da parte di soggetti incaricati facenti parte di una struttura che abbia in carico l'assistito.*

La cartella clinica elettronica*: collezione sistematica di informazioni sulla salute degli individui o di una popolazione in formato digitale.*

La profilazione*: qualsiasi forma di trattamento automatizzato di dati personali per valutare determinati aspetti personali relativi ad una persona fisica, come ad esempio il rendimento professionale, la salute, le preferenze personali, l'ubicazione o gli spostamenti della stessa.*

La pseudonimizzazione*: il trattamento dei dati personali in modo che gli stessi non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che queste ultime 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 (art. 4, n. 5, GDPR 679/16).*

Il titolare del trattamento*: 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.*

Il responsabile del trattamento*: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;*

Il referente del trattamento*: la persona fisica o giuridica, il servizio o altro organismo che, all'interno dell'azienda ed in relazione ad aree specifiche di competenza, tratta dati personali per conto del titolare del trattamento.*

L'autorizzato al trattamento*: la persona fisica o giuridica, il servizio o altro organismo che ha accesso consentito al trattamento dei dati personali in un ambito di attività puntualmente individuato, sotto l'autorità diretta del referente o del titolare del trattamento.*

L'interessato: *persona fisica cui si riferiscono i dati personali trattati.*

Il DPO (Data Protection Officer)*: la persona fisica o giuridica, il servizio o altro organismo nominato responsabile della protezione dei dati.*

Il destinatario*: la persona fisica o giuridica, il servizio o altro organismo che riceve comunicazione di dati personali, che si tratti o meno di soggetti terzi.*

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

L'informativa privacy: informazione messa a disposizione dell'interessato attraverso la quale questi è edotto circa le modalità e le finalità del trattamento dei dati personali.

Violazione dei dati personali (data breach)*: 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.*

La videosorveglianza*: controllo ambientale effettuato nei locali o nelle pertinenze aziendali mediante apparecchi audiovisivi che rilevano immagini in una certa area, con possibilità o meno di registrazione degli eventi che vi accadono*

***Blumatica**: software di gestione nomine e registri aziendale*

1)DATI TRATTATI

I Dati trattati dal Presidio Anna Torrgiani sono le informazioni personali (es. dati anagrafici, recapito, tessera sanitaria, codice fiscale, ecc.) e sensibili (es. informazioni sullo stato di salute) che riguardano i propri utenti. Tutti i dati che vengono trattati sono i minimi indispensabili per l'erogazione e la gestione delle prestazioni e dei servizi richiesti. Tutti i dati personali vengono trattati dal personale nel rispetto del segreto professionale, del segreto d'ufficio e dei diritti e delle libertà fondamentali di ogni persona, fisica o giuridica, nonché della dignità individuale, con particolare riferimento alla riservatezza, secondo i principi della normativa privacy. Il trattamento dei dati personali in ogni processo aziendale, pertanto, è improntato a principi di cui all'art. 5 del Regolamento UE 679/16 (GDPR). Tutto il personale designato ed incaricato, in base alla proprie mansioni, effettua il trattamento dei dati personali assicurandosi che gli stessi siano 1) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato; 2) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; 3) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati, nel rispetto del principio di minimizzazione del trattamento dei dati; 4) 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 ; 5) 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'ar.89 del GDPR ; 7) 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 .

Le figure designate ed incaricate al trattamento dal Titolare hanno l'obbligo di: operare in modo da garantire la riservatezza degli utenti nonché da assicurare che le informazioni sanitarie, rese agli stessi verbalmente (chiamata dei pazienti, indagine anamnestica, elaborazione diagnostica, colloqui con i familiari, etc.) o tramite supporto cartaceo (documenti sanitari), non siano percepibili o accessibili da parte di terzi non espressamente autorizzati dagli interessati; accedere ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti istituzionali assegnati**;**

TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI (dati relativi alla salute in ambito sanitario)

Il trattamento dei dati sulla salute è consentito in presenza di taluni requisiti specifici individuati all'art. 9 del Regolamento UE, nello specifico, come ribadito dal Garante Privacy le deroghe al divieto generale di trattare le cc.dd. "categorie particolari di dati", tra cui rientrano quelli sulla salute, sulla base delle quali è ammesso il trattamento di tali dati, sono ora da individuarsi nell'art. 9 del Regolamento che elenca una serie di eccezioni che rendono lecito il trattamento e che, in ambito sanitario, sono riconducibili, in via generale, ai trattamenti necessari per: − motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri (art. 9, par. 2,

lett. g) del Regolamento UE) , individuati dall'art. 2-sexies del Codice; − motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che preveda misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale (art. 9, par. 2, lett. i) ; − finalità di medicina preventiva, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali, "finalità di cura", sulla base del diritto dell'Unione/Stati membri o conformemente al contratto con un professionista della sanità, (art. 9, par. 2, lett. h) e par. 3 del Regolamento) effettuati da (o sotto la responsabilità di) un professionista sanitario soggetto al segreto professionale o da altra persona anch'essa soggetta all'obbligo di segretezza. Ciò non esclude che a seconda dello specifico trattamento effettuato, non possa ritenersi applicabile al caso concreto una delle altre deroghe previste dall'art. 9 del Regolamento.

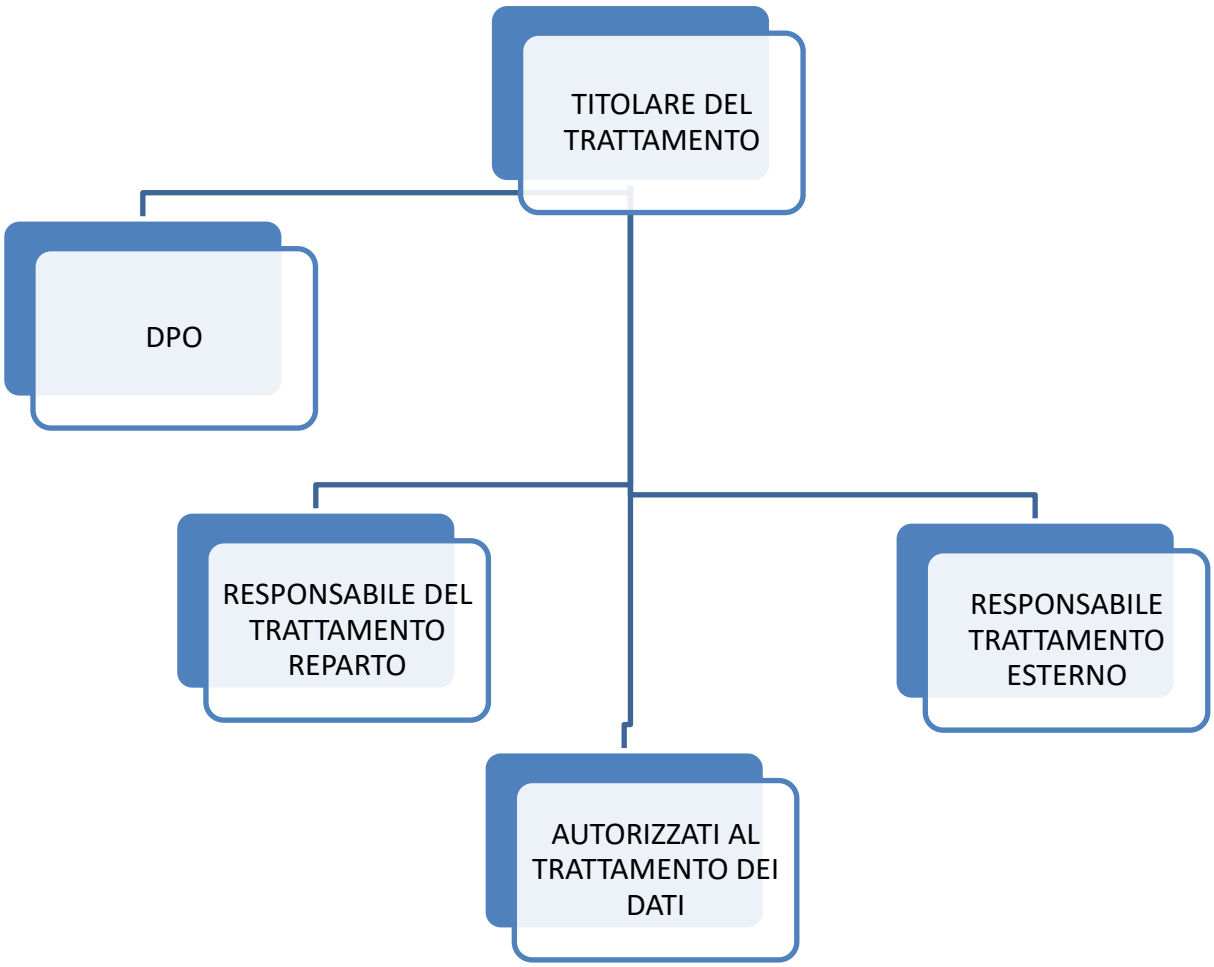
Al riguardo, si precisa che − I trattamenti per "finalità di cura", sulla base dell'art. 9, par. 2, lett. h) e par. 3 del Regolamento, sono propriamente quelli effettuati da (o sotto la responsabilità di) un professionista sanitario soggetto al segreto professionale o da altra persona anch'essa soggetta all'obbligo di segretezza.

− I trattamenti di cui all'art. 9, par. 2, lett. h) sono quelli "necessari" al perseguimento delle specifiche "finalità di cura" previste dalla norma, cioè quelli essenziali per il raggiungimento di una o più finalità determinate ed − esplicitamente connesse alla cura della salute (cfr. considerando 53 del Regolamento).

− Gli eventuali trattamenti attinenti, solo in senso lato, alla cura, ma non strettamente necessari, richiedono, quindi, anche se effettuati da professionisti della sanità, una distinta base giuridica da individuarsi, eventualmente, nel consenso dell'interessato o in un altro presupposto di liceità (artt. 6 e 9, par. 2, del Regolamento).

2. MODELLO ORGANIZZATIVO E SISTEMA GESTIONE DATI

Il Presidio Anna Torrigiani ha ritenuto necessario ridefinire all'assetto organizzativo per la gestione del Sistema aziendale di Protezione Dati personali, al fine di rispettare gli obblighi organizzativi, documentali e tecnici, con l'obiettivo di attuare la piena e consapevole applicazione del quadro normativo in materia di trattamento dei dati personali definito dal Regolamento UE n. 679/16 e del D.Lgs 101/2018. A tal fine il Titolare del trattamento ha determinato l'organigramma aziendale della Protezione Dati, descritto dettagliatamente nel seguito, con identificazione dei ruoli e delle responsabilità aziendali all'interno del Sistema di Gestione, al fine di garantire la conformità alle indicazioni del Regolamento UE in coerenza con l'attuale assetto organizzativo aziendale. Il sistema privacy verrà gestito con l'ausilio di un software dedicato.



3.I SOGGETTI PRIVACY

3.1 Il Titolare del Trattamento

Il Titolare del trattamento è il Presidio Torrigiani, nella persona del suo Direttore.

Il Titolare, cui competono le decisioni in ordine ai fini, alle modalità e ai mezzi del trattamento, ivi compreso il profilo della sicurezza, provvede alla corretta applicazione della normativa in materia di protezione dati.

Il Titolare provvede a nominare gli autorizzati al trattamento e a designare quali Responsabili del trattamento tutti i soggetti terzi che, in esecuzione di un contratto di fornitura o di una convenzione, effettuino un trattamento di dati personali per conto del Titolare stesso.

3.2 Il responsabile privacy

In applicazione di quanto disposto dal Regolamento UE e dal Codice Privacy in tema di profili di responsabilità e designazione dei soggetti autorizzati ad eseguire operazioni di trattamento di dati personali, avvalendosi dello strumento della delega, ha attribuito compiti e funzioni proprie ai Responsabili di Reparto.

In virtù dell'atto di delega il Titolare impartisce a tali soggetti le istruzioni e gli adempimenti connessi a una compiuta e corretta attività di protezione dei dati personali, tra i quali, secondo un elenco non esaustivo:

- fare osservare le istruzioni e le direttive aziendali in materia di protezione dati, fornite dal Titolare del trattamento.
- porre in atto all'interno della propria struttura organizzativa le procedure e le linee guida aziendali per la corretta gestione dei dati;
- vigilare sulla conformità dell'operato dei propri preposti alle istruzioni e alle direttive di cui sopra, verificando periodicamente lo stato di adeguamento alla normativa in oggetto;
- verificare che i dati oggetto di trattamento siano esatti, aggiornati, indispensabili, pertinenti e non eccedenti rispetto alle finalità per cui vengono trattati;
- attenersi alle indicazioni di sicurezza dettate dal Titolare del trattamento;
- compatibilmente con l'ambito di attività, adottare le misure di sicurezza tecniche e soprattutto organizzative adeguate, al fine di proteggere i dati da trattamenti non autorizzati o illeciti, dal rischio di perdita, di distruzione o di danno accidentale;
- partecipare ai momenti formativi organizzati dal presidio ed assicurare la partecipazione dei propri preposti;
- segnalare al Titolare ogni questione rilevante in materia e trasmettere tempestivamente istanze e reclami degli interessati;
- comunicare al Titolare i trattamenti in essere all'interno del proprio settore di competenza, l'inizio di ogni nuovo trattamento e la cessazione o modifica di quelli esistenti, ai fini dell'aggiornamento del Registro dei trattamenti aziendale;
- non realizzare trattamenti di dati diversi e ulteriori senza la preventiva autorizzazione del Titolare del trattamento;
- comunicare tempestivamente al Titolare i potenziali casi di data breach all'interno della propria struttura;

3.4 I soggetti autorizzati

Ai fini dell'autorizzazione al trattamento, prevista dall'art.2-quaterdecies del D.lgs.n.196/2003 e ss.mm.ii, si precisa che per personale autorizzato al trattamento dei dati s'intende tutto il personale dipendente del Presidio

Anna Torrigiani, nonché tutti coloro che, pur in assenza di un rapporto di lavoro dipendente, siano, a vario titolo, inseriti stabilmente all'interno dell'organizzazione ed effettuino operazioni di trattamento dei dati personali, ognuno per il proprio specifico ambito di competenza professionale, e che il personale già nominato incaricato di trattamento sia da considerarsi personale autorizzato al trattamento.

La nomina dei dipendenti e di coloro che, a diverso titolo, trattano i dati personali nel contesto della singola articolazione aziendale costituisce atto autorizzativo al relativo trattamento ai sensi degli articoli 29 del Regolamento UE e 2-quaterdecies del Codice.

Spetta all'amministrazione del Personale nominare i soggetti autorizzati al trattamento al momento della sottoscrizione del contratto individuale di lavoro, del contratto di collaborazione coordinata e continuativa, del contratto libero professionale, del contratto di borsa di studio, del tirocinio, del trasferimento e/o mutamento di mansioni. Contestualmente vengono fornite le istruzioni operative di carattere generale e particolare di cui sono invitati a prendere visione.

3.4 Il Responsabile esterno del trattamento

Il Responsabile del trattamento è la persona fisica o giuridica, autorità pubblica, servizio o altro organismo esterno rispetto al Presidio Anna Torrigiani che, in virtù di rapporti contrattuali o convenzionali tratta dati personali per conto del Titolare del trattamento.

3.5 Il Responsabile della protezione dei dati (DPO)

In applicazione dell'art. 37 del Regolamento UE, Il Presidio Anna Torrigiani provvede a nominare il proprio DPO, attribuendogli il ruolo e i compiti previsti dagli artt. 38 e 39 del Regolamento UE.

3.6 I Soggetti terzi

I soggetti terzi che accedono alla struttura, compresi i volontari, devono rispettare, in materia di privacy e di approccio agli ospiti, tutte le regole e le garanzie previste per il personale.

In ogni caso, è previsto per i soggetti esterni il divieto di effettuare fotografie e/o riprese video di persone ed ambienti senza preventivo formale assenso rispettivamente da parte degli interessati e dei responsabili di struttura.

4. IL TRATTAMENTO DEI DATI

4.1 Liceità del trattamento

I trattamenti dei dati personali che avvengono all'interno del Presidio Anna Torrigiani sono leciti e ricorre

sempre almeno una delle seguenti condizioni (art. 6 del GDPR):

- l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
- il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
- il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
- il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
- il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
- il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

I Referenti Privacy e/o i soggetti autorizzati sono tenuti a porre in essere ogni atto necessario per fornire agli interessati le informazioni di cui agli artt.13 e 14 del Regolamento UE, predisposte nel rispetto delle indicazioni fornite dal Titolare del trattamento e/o dal Responsabile della Protezione dei Dati.

4.2 Dati trattati e raccolta

Il Presidio Anna Torrigiani tratta dati personali relativi a:

- utenti, assistiti, pazienti e loro familiari e/o accompagnatori;
- personale sanitario, amministrativo, tecnico e professionale della dirigenza e del comparto con rapporto di dipendenza, convenzione o collaborazione;
- personale universitario che svolge attività assistenziale, di ricerca e di didattica all'interno dell'Azienda;
- soggetti che per motivi di studio, tirocinio, stage o volontariato frequentano le strutture dell'Azienda ed effettuano trattamento di dati personali, quali specializzandi, allievi tirocinanti, volontari;
- soggetti che intrattengono rapporti contrattuali con il Presidio Anna Torrigiani ai fini della fornitura di beni e servizi, attività di assistenza o consulenza, esecuzione di opere edilizie, interventi di manutenzione su software o dispositivi medici;
- soggetti e imprese partecipanti a bandi di gara o di pubblico concorso.

L'Azienda effettua il trattamento dei soli dati necessari per le finalità per le quali vengono raccolti o trattati tra cui:

- dati personali comuni quali: nome, cognome, residenza, cittadinanza, recapito telefonico, codice fiscale;

- categorie particolari di dati personali;
- dati economici quali: retribuzione, compensi, benefici, agevolazioni;
- dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza
- dati relativi ai familiari, quando richiesti da un presupposto di legge o di regolamento.

I dati personali trattati dal Presidio nelle forme e nei limiti di quanto previsto dalla vigente normativa sono raccolti:

- prioritariamente presso l'interessato o anche presso persone diverse nei casi in cui questi sia minorenne o incapace o non sia in grado di fornirli;
- presso enti del SSN, presso altri enti e amministrazioni pubbliche o terzi, presso pubblici registri o presso altri esercenti le professioni sanitarie.

Dati relativi alla salute – Esonero consenso

Il Presidio Anna Torrigiani tratta i dati personali relativi alla salute ai sensi dell'art.9 paragrafo 2 lettere h) ed i) del GDPR e dunque, senza necessità di raccogliere il consenso (sempre che non siano trattati dati genetici e/o biometrici), per le seguenti finalità:

- tutela della salute e dell'incolumità fisica (ossia attività di prevenzione, diagnosi, cura, assistenza, terapia sanitaria o sociale, riabilitazione), anche nell'ambito di percorsi di cura integrati che coinvolgano altri soggetti/ strutture sanitarie pubbliche o private;
- medicina preventiva;
- tutela dell'incolumità fisica e della salute di terzi e della collettività;
- medicina del lavoro e valutazione della capacità lavorativa dei dipendenti;
- motivi di interesse pubblico nel settore della sanità pubblica.

Il trattamento disciplinato dal presente articolo è indispensabile per l'erogazione e la gestione delle prestazioni sanitarie richieste ed è effettuato, nel pieno rispetto del segreto professionale, del segreto d'ufficio e secondo i principi della normativa privacy, da personale dipendente o da altri soggetti che collaborano con il Presidio Anna Torrigiani (ad es. medici in formazione specialistica, tirocinanti...) tutti debitamente designati ed a ciò autorizzati.

I dati relativi allo stato di salute non sono oggetto di diffusione ma possono essere comunicati, nei casi previsti da norme di legge o di regolamento, a soggetti pubblici e privati, enti ed istituzioni, per il raggiungimento delle rispettive finalità.

5. DIRITTI DEGLI INTERESSATI

Nella organizzazione delle prestazioni e dei servizi, Il Presidio Anna Torrigiani adotta misure di tipo organizzativo volte a garantire il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché

del segreto professionale. Il Presidio agevola l'esercizio dei diritti degli interessati nel rispetto dei principi di semplificazione e trasparenza.

Nello specifico, sono state individuate le misure procedurali disposte dal Titolare del trattamento per permettere all'utente interessato di ottenere in qualsiasi momento informazioni sull'utilizzo dei propri dati ai sensi degli artt.15-21 del Regolamento UE,

esercitando i diritti:

- di accesso (art.15);
- di rettifica (art.16);
- alla cancellazione (art.17);
- di limitazione del trattamento (art.18);
- alla portabilità dei dati (art.20);
- di opposizione al trattamento (art.21).

A tal fine, le richieste di accesso ai propri dati personali, di rettifica, aggiornamento, cancellazione, integrazione dei dati, nonché di opposizione al trattamento possono essere presentate al Presidio Anna Torriani all'indirizzo pec cr.toscana@cert.cri.it

Accesso alla documentazione sanitaria

Il Presidio applica quanto contenuto nell'art. 59 del D. Lgs. 196/2003 in materia di accesso a documenti amministrativi contenenti dati personali, disciplinato dalla L. 241/90, e di accesso civico, disciplinato dal D. Lgs. 33/2013. In osservanza delle richiamate disposizioni valuta caso per caso, anche con riguardo ad altre regolamentazioni specifiche, la possibilità da parte di terzi di accedere a documenti contenenti dati di cui agli articoli 9 e 10 del GDPR.

Invece, ai sensi dell'art. 60 del D. Lgs. 196/2003, quando il trattamento concerne dati genetici, relativi alla salute, alla vita sessuale o all'orientamento sessuale della persona, il trattamento è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi, è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale.

In particolare, in caso di richiesta di cartella clinica e di altri documenti sanitari ai fini della difesa in giudizio o ai sensi dell'art. 391quater c.p.p., ai fini della valutazione dell'ammissibilità e fondatezza della richiesta il difensore deve documentare la sua veste, anche mediante autocertificazione che individui gli estremi del procedimento nel quale svolga tale funzione e deve specificare le ragioni per le quali ritiene che le informazioni contenute nei documenti richiesti siano rilevanti per la finalità difensiva del proprio assistito, anche mediante

esibizione di documenti che ritenga all'uopo giustificativi.

Trasparenza e pubblicità legale

Ai sensi dell'art. 2-septies, comma 8, del D. Lgs. n. 196/2003, e dell'art. 7-bis, comma 6, del D. Lgs. n. 33/2013 è sempre vietata la diffusione di dati genetici, biometrici e relativi alla salute e alla vita sessuale.

Salvo diversa disposizione di legge, i documenti da pubblicare sul sito istituzionale per finalità di trasparenza e/o pubblicità legale non devono contenere in forma intelligibile dati personali non pertinenti o, se sensibili o giudiziari, non indispensabili rispetto alle finalità di trasparenza della pubblicazione.

Tra i dati da oscurare o rendere anonimi o da pseudonomizzare si citano, a titolo esemplificativo e non esaustivo: utenza telefonica e posta elettronica privati, indirizzi di residenza, codice fiscale, indicatore ISEE, carta d'identità o altra documentazione personale, numero di IBAN, dati relativi a condanne penali o reati, documentazione da cui si possa desumere, anche indirettamente, l'esistenza di patologie o condizioni di invalidità, disabilità, handicap fisici e/o psichici che riguardano l'interessato o familiari, documentazione da cui si evinca l'origine razziale ed etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, politico o sindacale. In tutti questi casi l'ufficio competente alla redazione e conservazione del documento, con la consulenza ove necessario del Responsabile della protezione dei dati, verifica, caso per caso, se esistano i presupposti per oscurare od omettere determinate informazioni prima della trasmissione all'ufficio deputato alla pubblicazione sul sito web aziendale.

Ulteriori misure operative sui diritti degli interessati

È fatto divieto a chiunque di fornire indicazioni inerenti lo stato di salute degli interessati per via telefonica o telematica.

Il Responsabile Privacy vigila che:

- le fotocopiatrici ed i fax siano collocati in un'area protetta e presidiata o che vengano utilizzati codici per il ritiro di copie e che il personale autorizzato presti attenzione alle fasi di invio e di ricevimento della documentazione contenente dati personali, non lasciandoli esposti alla visibilità di chiunque;
- nel caso si debba procedere alla comunicazione di dati particolari tramite fax con un ente esterno autorizzato per legge all'acquisizione di tale documentazione, laddove ne sia consentito l'utilizzo, si concordi un numero di fax non accessibile a terzi da utilizzare sempre e in modo esclusivo per tale comunicazione. Ciascuna comunicazione dovrà essere preceduta da una copertina nella quale non siano inclusi dati personali particolari né dati personali di soggetti diversi dal mittente e dal destinatario.

Il personale autorizzato al trattamento è tenuto al ritiro tempestivo della documentazione dalla stampante e dalla fotocopiatrice contenente dati personali ed alla conservazione della stessa. In tali casi è comunque fatto divieto di utilizzare supporti cartacei che contengano già informazioni personali e particolari sull'altro lato del foglio.

Il personale autorizzato che proceda alla eliminazione di stampe e fotocopie è tenuto a distruggere fisicamente i supporti in modo da impedire la ricostruzione o comunque da renderla non facilmente accessibile a terzi non autorizzati. La trasmissione interna ed esterna di corrispondenza e di documentazione contenente dati particolari deve essere effettuata necessariamente in busta chiusa e sigillata che riporti il nominativo del destinatario.

L'accesso alle immagini registrate dai sistemi di videosorveglianza è consentito nel rispetto di quanto previsto dalle linee guida in materia di Videosorveglianza.

Laddove necessario per finalità di diagnosi e terapia o per la corretta alimentazione del paziente, le domande relative alla convinzione religiosa dell'interessato devono essere formulate in modo generico tale da non arrecare pregiudizio e disagio allo stesso.

6. RICERCA E SPERIMENTAZIONI CLINICHE

Il Presidio Anna Torrigiani sostiene l'attività di ricerca e ne garantisce la gestione nel rispetto degli aspetti autorizzativi, normativo-regolatori e di protezione dei dati personali dei pazienti coinvolti. L'attività di ricerca si esplica previa specifica informativa da rendere agli interessati e previa raccolta del loro consenso, salve le deroghe sancite dall'Autorità Garante.

Infatti, ferma restando l'applicazione dell'art.104 e ss. del Codice, le informazioni di cui agli artt.13 e 14 del Regolamento UE devono essere fornite in modo tale da mettere in grado gli interessati di distinguere con le attività di ricerca da quelle di tutela della salute e, comunque, devono rendere edotto il paziente in modo chiaro ed inequivocabile che le informazioni contenute nella cartella clinica saranno utilizzate ed eventualmente comunicate ad una o più aziende farmaceutiche e/o produttrici di dispositivi medico sanitari e/o chirurgici o di altri Enti o altri committenti pubblici e privati, indicate nominativamente e se i dati comunicati lo rendono identificabile o sono resi anonimi.

E così, nello specifico agli interessati saranno sempre comunicate in maniera chiara e comprensibile tutte le informazioni riguardanti le modalità e i fini della ricerca.

In tale ambito il Titolare si avvale dello strumento della delega di funzioni, per attribuire le competenze e le responsabilità in materia di protezione dei dati personali e i relativi compiti, oltre a quelli ulteriori legati alla specifica attività, a ciascun Responsabile Scientifico volta per volta individuato nel provvedimento autorizzatorio per ciascun progetto di ricerca/sperimentazione clinica. Gli aspetti procedurali, amministrativi ed economici per la conduzione di ricerche e sperimentazioni cliniche sono definiti da apposito documento aziendale a cui si fa rinvio.

Il trattamento dei dati genetici è consentito nei soli casi previsti dall'art. 9, par. 2 del Regolamento UE, nonché

nel rispetto delle relative prescrizioni approvate dall'Autorità Garante nel Provvedimento del 5/6/2019 n. 146 che ha aggiornato, adeguandole al Regolamento UE, le prescrizioni di cui alla previgente n.8/2016 e delle misure di garanzia approvate dall'Autorità.

7. VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DATI (DPIA)

La Valutazione di impatto sulla protezione dati verrà eseguita dal Presidio soprattutto quando il trattamento "può presentare un rischio elevato per i diritti e le libertà delle persone fisiche".

Pertanto il Titolare del trattamento assicura l'esecuzione della valutazione secondo una metodologia standardizzata e ricorrendo al software di gestione dati personali , composta dalle fasi di seguito descritte.

Analisi ed individuazione dei trattamenti dati effettuati dalla azienda attraverso un'attenta mappatura dei processi e dei flussi informativi ad esso sottesi, con redazione del registro delle attività di trattamento.

- Identificazione sistemica della tipologia di trattamento, delle finalità di trattamento con classificazione della tipologia di dati trattati.
- Individuazione dei tempi di conservazione dei dati personali trattati nei singoli processi indicati nel registro delle attività di trattamento.
- Valutazione dell'adeguatezza, pertinenza e non eccedenza della tipologia e del numero dei dati trattati rispetto al raggiungimento della finalità prefissate.
- Identificazione e verifica delle modalità in cui il dato viene acquisito, elaborato, comunicato ed archiviato, secondo quanto previsto nel registro delle attività di trattamento.
- Valutazione e Verifica delle misure adottate dall'azienda per garantire il rispetto dei diritti degli interessati
- Individuazione, monitoraggio e revisione delle misure organizzative e tecniche utilizzate per mitigare il rischio con particolare riferimento alla trasmissione e all'archiviazione dei dati personali.

In particolare per ogni trattamento sono controllate e valutate le seguenti misure di sicurezza:

- Misure di sicurezza organizzative;
- Misure di sicurezza applicate ai dati;
- Misure di sicurezza applicate ai sistemi.

Valutazione del Rischio Residuo a termine di Valutazione d'impatto basato su:

- Determinazione dell'origine, natura, particolarità e gravità dei rischi (accesso illegittimo, modifica indesiderata e scomparsa dei dati, etc..)
- Stima della probabilità di accadimento dell'evento avverso e della gravità del danno causato per i diritti fondamentali dell'Interessato;
- Determinazione delle misure aggiuntive previste per gestire i rischi individuati

8. DATA BREACH O VIOLAZIONE DEI DATI PERSONALI

In caso di violazione dei dati personali (c.d data breach), anche potenziale, si applica la procedura adottata dal Presidio Anna Torrigiani in conformità agli artt.33 e 34 del Regolamento UE, al fine di tutelare le persone, i dati e le informazioni e di documentare i flussi per la gestione delle violazioni dei dati personali.

La procedura definisce i ruoli e le funzioni dei soggetti coinvolti nella valutazione e graduazione del rischio della eventuale violazione e le fasi istruttorie conseguenti.

L'intero iter di gestione della segnalazione viene documentato dal DPO nel Registro Aziendale delle Violazioni.

9. REGISTRO DELLE ATTIVITA' DI TRATTAMENTO

Il titolare del trattamento tiene un registro delle attività di trattamento svolte sotto la propria responsabilità, contenente le informazioni di cui all'art. 30, paragrafo 1, del GDPR:

- il nome e i dati di contatto del titolare del trattamento e del responsabile della protezione dei dati;
- le finalità del trattamento;
- una descrizione delle categorie di interessati e delle categorie di dati personali;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
- i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale;
- i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- una descrizione generale delle misure di sicurezza tecniche e organizzative.

Ogni responsabile del trattamento tiene un registro di tutte le categorie di attività relative al trattamento svolte per conto del titolare, contenente le informazioni di cui all'art. 30, paragrafo 2, del GDPR.

10. FORMAZIONE

Il Presidio Anna Torrigiani mette in atto la formazione del personale un elemento strategico della propria politica in materia di protezione dei dati personali. Pertanto il Titolare del trattamento, per il tramite del Responsabile della UO Qualità e Formazione, assicura il mantenimento di programmi di formazione specifici in materia di Privacy da effettuare ai Responsabili designati e a tutto il personale incaricato al trattamento dei dati personali, al fine di garantire che il personale abbia un approccio consapevole sui rischi e sulle misure di sicurezza tecnico organizzative e per diffondere la sensibilità a livello aziendale sui temi legati alla tutela della privacy e alla protezione dati.

11. VERIFICHE PERIODICHE

Il Titolare, tramite verifiche periodiche affidate al Responsabile per la Protezione dei Dati (DPO) e/o ad altro soggetto in possesso di comprovate capacità professionali, effettua attività di audit, intesa come attività di controllo interno volta a verificare la conoscenza delle procedure aziendali, e i controlli opportuni per vigilare sulla puntuale osservanza della normativa vigente. Gli Audit interni, previste nel presente documento, prevedono le seguenti fasi:

1) verifica della gestione documentale del sistema, con particolare riferimento alla tenuta, aggiornamento ed archiviazione dei Registri previsti nelle procedure del Sistema;
2) monitoraggio dei processi relativi ai trattamenti dati determinati all'interno del Registro delle attività di trattamento, con eventuale aggiornamento dello stesso;
3) verifica della efficacia delle misure di sicurezza organizzative e tecniche adottate dal Titolare per il tramite dei Responsabili designati al trattamento;
4) analisi delle eventuali anomalie e criticità riscontrate, con individuazione delle opportune azioni preventive e correttive mirate al miglioramento di un intero processo o di uno specifico trattamento

12. SISTEMI DI VIDEOSORVEGLIANZA

L'installazione di apparecchiature di videosorveglianza è autorizzata dal Presidio Anna Torrigiani nel rispetto delle disposizioni vigenti, solo quando ciò sia strettamente indispensabile per garantire la sicurezza del patrimonio aziendale e delle persone che, a vario titolo, accedano alle strutture aziendali.

Il trattamento dei dati personali effettuato attraverso i sistemi di videosorveglianza avviene nel rispetto della dignità e dell'immagine delle persone, delle norme a tutela dei lavoratori (art. 4 L. 300/1970 s.m.i.) e dei Provvedimenti in materia emessi dall'Autorità Garante per la protezione dei dati personali.

13. CONCLUSIONI

In caso di dubbi sulla applicazione della normativa in materia di protezione dei dati personali e delle presenti linee guida il personale autorizzato è tenuto ad attenersi al criterio della tutela e del massimo rispetto della riservatezza nei confronti dell'interessato, pur garantendo allo stesso tempo il normale espletamento delle attività. Per tutto quanto non espressamente previsto dal presente documento si rinvia alle disposizioni europee, nazionali, regionali ed aziendali in materia.