REGOLAMENTO AZIENDALE PER LA GESTIONE E LA PROTEZIONE DEI DATI PERSONALI

Sommario

Premesse 2
Contesto 2
La normativa in materia di protezione dati personali – caratteri generali 2
Strutture preposte al trattamento dei dati personali nell'ambito dell'Ospedale di Sassuolo S.p.A. ... 3
Il Titolare del trattamento 3
Il Direttore Generale 3
Il Registro delle attività di trattamento 4
I soggetti designati: il nuovo modello organizzativo in tema di protezione dati 4
I Delegati al trattamento dei dati 5
Gli Autorizzati al trattamento dei dati 6
Referente Aziendale Protezione dei dati personali 6
Responsabile del trattamento 7
Il Responsabile della protezione dei dati personali (DPO) 7
Aspetti specifici 8
Misure di sicurezza tecniche e ruolo del SIA e Ingegneria Clinica 8
Amministratore di Sistema 9
Misure di sicurezza dei documenti e degli archivi cartacei 9
Misure di sicurezza organizzative per il rispetto della dignità' degli interessati 10
Procedura per la segnalazione di violazioni di dati 10
Informazioni agli interessati 10
Esercizio dei diritti degli interessati 11
Accesso alla documentazione sanitaria 11
Ricerca e sperimentazioni cliniche 12
Dati genetici 12
Dossier sanitario elettronico aziendale 12
Trattamento di dati personali per finalità di trasparenza e pubblicità legale 13
Libera Professione 13
Sistemi di videosorveglianza 13

Rinvio a norme e provvedimenti aziendali per specifici settori 13
Entrata in vigore del Regolamento e forme di pubblicità 13
Allegati 14
Allegato 1: organigramma 14
Allegato 2: compiti del delegato al trattamento 14
Allegato 3: atto di designazione del soggetto autorizzato al trattamento 14

Premesse

Contesto

L'Ospedale di Sassuolo S.p.A. (in seguito anche "Società" o "Ospedale di Sassuolo") è una struttura sanitaria formalmente autorizzata in via sperimentale con deliberazione della Giunta Regionale dell'Emilia Romagna n. 1337/2002 e successivamente convertita in regime ordinario con deliberazione della Giunta Regionale dell'Emilia Romagna n. 102/2009, in conformità all'art. 9bis del D. Lgs. 502/1992 e s.i.m. La Società è costituita con Atto Costitutivo del 21/10/2002. L'Ospedale di Sassuolo S.p.A. si configura come una "società a partecipazione pubblica", a capitale misto e a maggioranza pubblica, che prevede la partecipazione maggioritaria dell'Azienda USL di Modena ed è stato accreditato con Determinazione del Direttore Generale Sanità e Politiche Sociali n.12862/2012. All'interno del Servizio Sanitario Regionale, di cui è parte, l'Ospedale persegue una mission pubblica ed opera nel rispetto delle condizioni e della programmazione definita a livello regionale e locale, integrandosi nella rete dei servizi ospedalieri e territoriali presenti sul territorio modenese.

La normativa in materia di protezione dati personali – caratteri generali

Il "Regolamento Europeo 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati" (di seguito "GDPR"), detta una complessa disciplina di carattere generale in materia di protezione dei dati personali, prevedendo molteplici obblighi e adempimenti a carico dei soggetti che trattano dati personali. Le disposizioni della normativa nazionale, ovvero il D. Lgs. 196/2003 "Codice in materia di protezione dei dati personali" e i Provvedimenti di carattere generale adottati dall'Autorità di controllo italiana (Garante per la protezione dei dati personali) trovano applicazione nella misura in cui non siano in contrasto con la normativa europea. Il GDPR affronta il tema della tutela dei dati personali attraverso un approccio nuovo, basato principalmente sulla valutazione dei rischi riguardanti i diritti e le libertà degli interessati e attribuisce ai Titolari del trattamento il compito di assicurare ed essere in grado di comprovare il rispetto dei principi applicabili al trattamento dei dati personali, adottando le misure che ritiene a ciò più idonee ed opportune (c.d. principio di responsabilizzazione o accountability).

Il GDPR definisce:

- all'art. 4, n. 7) il Titolare del trattamento come "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 Titolare dunque decide rispettivamente il "perché" e il "come" del trattamento, vale a dire rispettivamente, il motivo per il quale ha inizio un trattamento e le modalità con le quali il trattamento stesso deve essere svolto per raggiungere l'obiettivo;
- all'art. 4 n. 2 il trattamento come "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".

Strutture preposte al trattamento dei dati personali nell'ambito dell'Ospedale di Sassuolo S.p.A.

Il Titolare del trattamento

Alla luce delle premesse sopra illustrate, ai fini della applicazione della normativa in materia di protezione dei dati personali, l'Ospedale di Sassuolo S.p.A., nello svolgimento di tutte le proprie attività istituzionali e nel perseguimento della propria mission si configura pertanto come autonomo Titolare del trattamento ai sensi degli artt. 4, n. 7) e 24 del GDPR.
Al fine di garantire l'attuazione degli adempimenti previsti dalla normativa di settore, con il presente documento l'Ospedale di Sassuolo S.p.A. definisce il proprio ambito di titolarità e il complessivo riparto delle responsabilità in tema di trattamento dati, indica i compiti assegnati al Responsabile della Protezione dei Dati (DPO) designato, detta i criteri generali da rispettare nell'individuazione dei soggetti autorizzati a compiere le operazioni di trattamento e relativi compiti e istruzioni.

Il Direttore Generale

Il Consiglio di Amministrazione delega il Direttore Generale a compiere ogni atto utile al fine di garantire, ed essere in grado di dimostrare, che il trattamento di dati personali effettuato dall'Ospedale è conforme al GDPR.
Al Direttore Generale dell'Ospedale di Sassuolo S.p.A./Titolare del trattamento, cui è conferita la rappresentanza legale nell'ambito dei compiti di gestione ed organizzazione attribuiti, è assegnato il compito di definire la politica di gestione per la corretta protezione dei dati personali durante tutte le fasi del loro trattamento e di individuare le misure tecniche e organizzative di sicurezza da adottare, al fine di garantire che il trattamento dei dati personali degli interessati all'interno dell'Ospedale (pazienti, utenti e dipendenti) avvenga nel rispetto dei principi generali di cui agli artt. 5 e ss. del GDPR;

In particolare spetta al Direttore Generale o a personale dallo stesso delegato:

- designare il DPO di cui agli artt. 37- 39 del Regolamento UE 2016/679 specificando i compiti allo stesso assegnati;
- attribuire funzioni e compiti, connessi al trattamento dei dati personali, a persone fisiche espressamente designate che operano sotto la responsabilità del Titolare, attraverso l'adozione di uno specifico organigramma (Allegato n. 1) e di uno specifico Regolamento aziendale;
- designare i Responsabili del trattamento di cui all'art. 28 del GDPR stipulando il contratto o l'atto giuridico di cui al medesimo art. 28, par. 3 e 4;
- approvare le policy aziendali e mettere in atto le misure tecniche e organizzative necessarie a garantire il livello di sicurezza adeguato al rischio di cui all'art. 32 del GDPR;
- approvare documenti organizzativi finalizzati a fornire le informazioni di cui agli artt. 13 e ss. del Regolamento, alla raccolta del consenso eventualmente necessario e a garantire i diritti degli interessati di cui agli artt. 15 e seguenti del medesimo GDPR;
- garantire la predisposizione e l'aggiornamento del Registro delle attività ai sensi degli artt. 30 e ss. del Regolamento;
- provvedere, se necessario, alla valutazione d'impatto ai sensi dell'art. 35 del Regolamento e alla eventuale successiva consultazione preventiva ai sensi dell'art. 36 del medesimo;
- allocare adeguate risorse per la formazione dei dipendenti, dei collaboratori e in generale di tutto il personale autorizzato al trattamento, in materia di protezione dei dati e sicurezza informatica;
- disporre periodiche verifiche sul rispetto delle funzioni impartite con riguardo agli aspetti relativi alla sicurezza dei dati e alla formazione (attività di audit interno e verso i responsabili del trattamento);
- provvedere alle notifiche e alle comunicazioni di cui agli artt. 33 e 34 del Regolamento (data breach);
- sottoscrivere, se ritenuto necessario, l'atto interno di cui all'art. 26 del Regolamento UE 2016/679 (in tema di contitolarità);
- favorire l'adesione a Codici di condotta ai sensi dell'art. 40 del Regolamento e a meccanismi di certificazione ai sensi dell'art. 42 del Regolamento;
- assolvere agli obblighi nei confronti del Garante per la protezione dei dati personali nei casi previsti dalla normativa.

Il Registro delle attività di trattamento

L'Ospedale redige, conserva e aggiorna il Registro delle attività di trattamento che contiene la rilevazione di tutti i trattamenti di dati personali che vengono in essere nello svolgimento della propria attività istituzionale ed è obbligatorio per tutti i titolari di trattamento, ai sensi dell'art. 30 del Regolamento Europeo. Il Registro è depositato presso il Referente Aziendale Privacy, a disposizione dell'Autorità Garante per la protezione dei dati personali.

I soggetti designati: il nuovo modello organizzativo in tema di protezione dati

Ai sensi dell'art. 32 del GDPR, al Titolare del trattamento competono le decisioni atte a garantire la sicurezza del trattamento dei dati personali, "tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche"; a tal fine il Titolare del trattamento mette in atto "misure tecniche ed

organizzative adeguate per garantire un livello di sicurezza adeguato al rischio", tra le quali rientra anche, richiamando quanto già previsto dall'art. 29 del GDPR, la previsione secondo cui chiunque agisca sotto l'autorità del Titolare del trattamento e abbia accesso a dati personali può trattare tali dati solo se adeguatamente istruito.

Alla luce di tali premesse, si rende necessario:

- determinare il modello organizzativo dell'Ospedale di Sassuolo S.p.A. in tema di protezione dati e i connessi livelli di responsabilità;
- definire di conseguenza un organigramma delle responsabilità privacy aziendali, sia in termini di professionisti coinvolti, che di attribuzioni di compiti e funzioni;
- infondere nell'organizzazione aziendale la piena consapevolezza dei rischi inerenti ai trattamenti, nonché l'affermazione di una cultura della protezione dei dati, quale parte integrante dell'intero asset informativo di un'organizzazione, con particolare attenzione ai dati di salute;
- coinvolgere tutti i soggetti chiamati a trattare i dati personali all'interno della organizzazione, con assunzione delle relative responsabilità, distinguendo tra Soggetti Delegati al trattamento (ex responsabili interni di trattamento) e Soggetti Autorizzati (ex incaricati).

I Delegati al trattamento dei dati

In considerazione della natura gestionale e della complessità delle strutture organizzative in termini di attività di trattamento dati e di personale assegnato, sono designati Delegati al trattamento i dirigenti individuati nell'organigramma privacy (Allegato 1), che di norma corrispondono ai Direttori di Unità Operativa, ai Responsabili di Struttura o di Funzione, al Responsabile delle Professioni Sanitarie. La attribuzione ai Delegati del trattamento così definiti di compiti e funzioni connessi al trattamento di dati personali avviene, appunto, avvalendosi dello strumento della delega per effetto dell'incarico ricoperto e senza necessità di nomina ad personam. La delega si esplica in particolare nello svolgimento dei compiti indicati nell'Allegato 2 al presente Atto, la cui elencazione non può comunque ritenersi esauriente rispetto a tutti i compiti e gli adempimenti connessi ad una compiuta e corretta attività di protezione dei dati.

Tale delega è condizionata alla durata dell'incarico e si intende revocata di diritto alla cessazione dell'incarico medesimo, fermo restando in ogni caso la facoltà del Direttore Generale, in qualità di Titolare del trattamento dei dati, di ritirarla in caso di inadempimento dei compiti assegnati avocando pertanto a sé le relative funzioni; inoltre, al fine di conferire continuità alle suddette responsabilità, la delega si estende ai dirigenti che, in caso di vacanza del ruolo del soggetto delegato, assumano la relativa responsabilità ad interim. Successivamente alla adozione del presente Atto, per i professionisti che assumano il ruolo per il quale è prevista la delega come da organigramma, la delega di funzioni opererà contestualmente alla sottoscrizione del relativo contratto di incarico, il quale viene pertanto adeguatamente integrato con indicazione dei relativi compiti e adempimenti e che il dipendente

interessato sottoscriverà per ricevuta. Infine, ai Delegati al trattamento come sopra individuati è riconosciuta la responsabilità del rilascio delle abilitazioni agli applicativi informatici aziendali.

Gli Autorizzati al trattamento dei dati

Si definiscono Autorizzati al trattamento dei dati personali di titolarità aziendale tutti i soggetti che operano sotto la diretta autorità del Titolare o del Delegato; si tratta pertanto di tutti i dipendenti/collaboratori della Società, nonché di tutti i titolari di lavoro autonomo se ed in quanto operanti stabilmente nell'ambito delle strutture aziendali. Nello specifico:

- dipendenti a tempo indeterminato e determinato
- borsisti
- liberi professionisti che operano stabilmente nell'Ospedale
- specializzandi
- interinali

Tali soggetti sono designati individualmente per iscritto e a loro si attribuisce la qualifica di "soggetti Autorizzati" al trattamento dei dati con riferimento allo specifico ambito di competenza professionale e ai trattamenti cui sono addetti, secondo quanto risulta dal registro dei Trattamenti di titolarità aziendale. I soggetti Autorizzati al trattamento sono tenuti alla osservanza delle istruzioni impartite dalla Società per il corretto trattamento dei dati personali contenute nell'atto di designazione (Allegato 3), oltre ad ulteriori istruzioni che il Titolare del trattamento, anche per il tramite dei Delegati, conferirà loro con riferimento a particolari trattamenti di dati (es. in caso di sperimentazioni o trattamento di dati genetici). Detta autorizzazione deve essere comunicata e recepita da tutti gli operatori sopra descritti mediante pubblicazione del presente documento e delle Istruzioni di carattere generale impartite dal Titolare, o dal Delegato. Per il personale di nuova assunzione, l'autorizzazione al trattamento dei dati viene fornita contestualmente alla sottoscrizione del relativo contratto di lavoro, il quale viene pertanto adeguatamente integrato con il predetto atto di designazione che il dipendente interessato sottoscriverà per ricevuta. Infine, il Delegato al trattamento provvederà di volta in volta a nominare "Autorizzato al trattamento" il personale non operante stabilmente nell'Ospedale e per il quale dunque l'autorizzazione al trattamento dei dati personali non può essere rilasciata contestualmente alla sottoscrizione di un contratto di lavoro/incarico (es. tirocinanti, studenti, stagisti frequentatori volontari, servizio civilisti, lavoratori socialmente utili etc.).

Referente Aziendale Protezione dei dati personali

Il Referente Aziendale Privacy, in attuazione dei principi di informazione e sensibilizzazione richiamati dal GDPR, ha il compito di assicurare un presidio aziendale per quel che concerne gli adempimenti organizzativi e procedurali derivanti dalle disposizioni normative in materia di protezione dei dati personali.

In particolare, il Referente Aziendale Privacy ha i seguenti compiti:

- supportare la Direzione aziendale attraverso la redazione di atti, regolamenti e istruzioni operative finalizzati al corretto trattamento dei dati, attraverso il monitoraggio sulla loro corretta applicazione e, più in generale, sulla corretta interpretazione e applicazione delle disposizioni normative vigenti;
- supportare i Delegati al trattamento nell'adozione delle misure adeguate ed efficaci per la tutela della riservatezza, integrità e disponibilità del patrimonio informativo, anche a seguito degli approfondimenti e delle analisi effettuate unitamente al DPO e ai Referenti Privacy delle altre Aziende Sanitarie presenti nel territorio della provincia di Modena;
- conservare e garantire l'aggiornamento del Registro dei trattamenti aziendale;
- fornire supporto alle verifiche di sicurezza svolte dal SIA e/o dal DPO;
- coordinare le richieste di parere al DPO da parte dei singoli Delegati al trattamento;
- coordinare le notifiche di violazione dei dati personali;
- assicurare, all'interno della società, un adeguato livello di formazione/informazione e predisporre e aggiornare i documenti aziendali in tema di privacy e sicurezza informativa e le informative aziendali.

Responsabile del trattamento

IL GDPR disciplina espressamente la figura del "Responsabile del trattamento" intendendosi con questa espressione i soggetti esterni alla organizzazione che trattano dati personali per conto del Titolare del trattamento. Tali soggetti devono presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento da loro posto in essere soddisfi i requisiti del GDPR e garantisca la tutela dei diritti degli interessati. A tal fine l'art. 28 del GDPR dispone che i trattamenti da parte di un Responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico che vincoli il Responsabile del trattamento al Titolare del trattamento e che definisca la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del Titolare del trattamento. Si attribuisce al Servizio Acquisti e Forniture, il cui Responsabile è designato Delegato al trattamento, qualora per lo svolgimento delle attività istituzionali sia necessario avvalersi di soggetti esterni alla Società e tali attività comportino il trattamento di dati personali per conto del Titolare del trattamento, il compito di provvedere alla contestuale stipula o predisposizione del relativo atto di designazione di tali soggetti esterni quali "Responsabili del trattamento", a norma dell'art. 28 del GDPR e delle condizioni ivi indicate. Tale attività è propedeutica all'aggiornamento del Registro aziendale delle attività di trattamento dei dati.

Il Responsabile della protezione dei dati personali (DPO)

Il GDPR prevede l'obbligo per il Titolare del trattamento di designare il Responsabile della protezione dei dati (RPD) o Data Protection Officer (DPO) tra gli altri casi, quando "il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico" o "le attività principali del titolare del trattamento […] consistono nel trattamento, su larga scala, di categorie

particolari di dati personali di cui all'articolo 9; tale obbligo pertanto si delinea anche in capo all'Ospedale di Sassuolo S.p.A..

In attuazione dell'art. 39 del GDPR il DPO ha il compito di:

- informare e fornire consulenza in ordine agli obblighi derivanti dal GDPR, nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati. Per il tramite del Direttore Generale dovrà altresì assicurare attività di informazione/consulenza ai Delegati al trattamento e ai soggetti Autorizzati che eseguono operazioni di trattamento dati;
- sorvegliare l'osservanza della normativa in materia di protezione dei dati personali nonché delle policy aziendali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti;
- fornire, se richiesti, pareri anche scritti in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
- cooperare con l'Autorità Garante per la protezione dei dati personali, fungendo da punto di contatto per la stessa per questioni connesse al trattamento (tra cui la consultazione preventiva) ed effettuare eventuali consultazioni e curarne in generale i rapporti;
- supportare la struttura deputata alla tenuta del Registro del trattamento;
- promuovere iniziative congiunte tra Ospedale di Sassuolo S.p.A. e altre Aziende Sanitarie, in particolare della stessa provincia o di Area Vasta, affinché l'applicazione della normativa in materia di protezione dei dati personali nonché delle policy aziendali sia sviluppata secondo linee applicative omogenee e coerenti;

Il DPO nello svolgimento dei compiti di cui sopra si avvale del Responsabile dell'ICT e del Referente Aziendale Privacy, quali primari interlocutori presso la Società.

Aspetti specifici

Misure di sicurezza tecniche e ruolo del SIA e Ingegneria Clinica

Il Sistema Informativo Aziendale (SIA) e il Servizio di Ingegneria Clinica, nell'ambito delle rispettive attività istituzionali, collaborano con il Referente Aziendale Privacy e con il Responsabile della Protezione dei Dati allo svolgimento dei seguenti compiti:

- adottare misure di sicurezza tecniche adeguate al fine di assicurare l'integrità e la disponibilità dei dati e di garantire la protezione dei dispositivi e dei programmi contro il rischio di intrusione o perdita e il tempestivo ripristino dei dati personali in caso di incidente;
- collaborare alla redazione e all'aggiornamento del Registro delle attività di trattamento, unitamente alla Direzione Sanitaria;
- procedere alla valutazione di impatto privacy di cui all'articolo 35 del Regolamento UE, avvisando il Titolare laddove rilevi la necessità di procedere alla consultazione preventiva al Garante, come previsto dall'articolo 36 del Regolamento UE.

Tra le funzioni proprie del SIA, connesse al corretto trattamento dei dati personali, rientrano anche:

- supporto all'Ingegneria Clinica per la corretta definizione degli aspetti di protezione dei dati personali riguardanti i dispositivi certificati come "Medical Device" (ai sensi della direttiva 93/42/EEC e s.m.i. e del Regolamento (UE) 2017/745);
- vigilanza sul rispetto del "Disciplinare" interno sull'utilizzo degli strumenti informatici.

Tutti gli operatori di SIA e SIC sono autorizzati al trattamento dei dati personali e sono pertanto tenuti al rispetto delle istruzioni indicate all'Art. 5 del presente Regolamento e del Disciplinare interno in materia di uso degli strumenti informatici; inoltre, a taluni di essi, espressamente individuati, i Responsabili dei suddetti Servizi possono attribuire la qualifica di "superutenti", ovvero utenti in possesso di particolari privilegi per intervenire sui sistemi aziendali al fine di garantirne operatività e sicurezza.

Amministratore di Sistema

Al fine di adempiere agli obblighi di maggiore controllo e responsabilizzazione imposti dal GDPR, secondo un'ottica di prevenzione del rischio, in relazione ai dati personali trattati con strumenti informatici, il Titolare o Suo delegato individua tra i dipendenti dell'Ospedale di Sassuolo S.p.A. l'Amministratore di Sistema nominandolo con apposito atto e fornendogli le necessarie istruzioni operative, in conformità al Provvedimento dell'Autorità Garante del 27 Novembre 2008. L'Amministratore di Sistema viene dunque preposto alla sicurezza, gestione e manutenzione di banche dati, sistemi e infrastrutture informatiche.

Misure di sicurezza dei documenti e degli archivi cartacei

Con riferimento al trattamento di dati personali su supporto cartaceo, i soggetti autorizzati devono attenersi al rispetto delle seguenti misure di sicurezza:

- conservare i documenti in luoghi e contenitori (armadi o cassetti chiusi a chiave, cassaforte, ecc.) atti ad evitare perdite, sottrazioni, danneggiamenti, distruzioni e accesso a soggetti non autorizzati; ove si utilizzi un contenitore/locale chiuso a chiave occorre accertarsi che non esistano duplicati abusivi delle chiavi e che le stesse siano in possesso solo di operatori autorizzati;
- per tutto il periodo in cui si effettuano le operazioni di trattamento dei dati, non perdere mai di vista i documenti, adempiendo ad un preciso obbligo di custodia dei medesimi;
- in caso di abbandono, anche temporaneo, dell'ufficio, non lasciare incustoditi i documenti (sulla scrivania o su tavolini di reparto).

L'accesso agli archivi aziendali è controllato. La responsabilità della conservazione e della sicurezza degli archivi amministrativi contenenti dati personali e allocati in locali siti all'interno della Struttura ricade sul Responsabile del servizio/Struttura che li produce e detiene, fino al loro conferimento all'archivio di deposito. La responsabilità della conservazione e della sicurezza delle cartelle cliniche e della documentazione sanitaria è in capo ai Direttori delle

rispettive Unità Operative, fino al loro conferimento all'archivio di deposito. Della corretta gestione, conservazione e della sicurezza di tale archivio risponde il soggetto terzo a cui l'archivio è affidato in outsourcing.

Misure di sicurezza organizzative per il rispetto della dignità' degli interessati

Nella organizzazione delle prestazioni e dei servizi, l'Ospedale adotta misure di tipo organizzativo volte a garantire il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale. Tali misure comprendono, ad esempio:

- soluzioni volte a rispettare, in relazione a prestazioni sanitarie o ad adempimenti amministrativi preceduti da un periodo di attesa, un ordine di precedenza e di chiamata degli interessati prescindendo dalla loro individuazione nominativa;
- l'istituzione di appropriate distanze di cortesia, tenendo conto dell'eventuale uso di apparati vocali o di barriere e della situazione logistica;
- soluzioni tali da prevenire, durante i colloqui, l'indebita conoscenza da parte di terzi di informazioni idonee a rivelare lo stato di salute;
- cautele volte ad evitare che le prestazioni sanitarie, ivi compresa l'eventuale documentazione di anamnesi, avvenga in situazioni di promiscuità derivanti dalle modalità o dai locali prescelti;
- il rispetto della dignità dell'interessato in occasione della prestazione medica e in ogni operazione di trattamento dei dati;
- la previsione di opportuni accorgimenti volti ad assicurare che, ove necessario, possa essere data correttamente notizia o conferma anche telefonica solo ai terzi legittimati (come parenti, familiari, conviventi, conoscenti, personale volontario) della presenza di una persona al pronto soccorso o in un reparto di degenza;
- la messa in atto di procedure, anche di formazione del personale, dirette a prevenire nei confronti di estranei un'esplicita correlazione tra l'interessato e reparti o strutture sanitarie, indicativa dell'esistenza di particolari patologie o stati di salute.

Procedura per la segnalazione di violazioni di dati

In ottemperanza a quanto disposto dall'art. 33 del Regolamento UE, l'Ospedale ha adottato la procedura per la rilevazione e la gestione - e la eventuale notifica entro i termini all'Autorità Garante e agli interessati - dei casi di violazione di dati personali (c.d. data breach) e per la tenuta del relativo registro delle violazioni, depositato presso l'Ufficio Privacy Aziendale.

Informazioni agli interessati

Nell'ambito delle attività di trattamento dei dati personali necessarie per lo svolgimento delle proprie attività istituzionali, il Titolare fornisce agli interessati tutte le informazioni previste dagli artt.13 e 14 del Regolamento UE. Le predette informazioni sono fornite attraverso una informativa generale, distribuita presso tutte le Unità Operative e i Servizi dell'Ospedale, mediante affissione nei punti di accesso al pubblico, ben visibili all'utenza, nonché pubblicata nella sezione Privacy del sito internet aziendale.

Le informazioni da rendere per trattamenti di dati necessari per l'esecuzione di un contratto di cui l'interessato è parte (o di misure precontrattuali adottate su richiesta dello stesso) e per assolvere agli obblighi del Titolare nell'ambito del rapporto di lavoro sono inserite nei relativi atti contrattuali e, laddove siano previste procedure concorsuali, dovranno essere necessariamente contenute nei bandi di concorso, di gara, nelle lettere di invito e/o avvisi pubblici.

Inoltre, specifiche note informative relative a particolari attività di trattamento sono predisposte e rese solo agli utenti/pazienti effettivamente coinvolti, ad esempio in caso di sperimentazioni e ricerca clinica.

Le informazioni in merito al trattamento dei dati personali sono fornite successivamente alla erogazione della prestazione sanitaria in caso di:

- emergenza sanitaria o di igiene pubblica per la quale la competente autorità ha adottato un'ordinanza contingibile e urgente;
- impossibilità fisica, incapacità di agire o incapacità di intendere o di volere dell'interessato, quando non sia possibile renderle a chi esercita legalmente la rappresentanza, ovvero a un prossimo congiunto, a un familiare, a un convivente o unito civilmente ovvero a un fiduciario ai sensi dell'art. 4 della L. 219/2017 o, in loro assenza, al responsabile della struttura presso cui dimora l'interessato;
- rischio grave, imminente ed irreparabile per la salute o l'incolumità fisica dell'interessato;
- prestazione medica che può essere pregiudicata dal loro preventivo rilascio, in termini di tempestività o efficacia.

All'obbligo di fornire sempre agli interessati le informazioni sul trattamento dei loro dati personali, non corrisponde più analogo obbligo per le strutture sanitarie di acquisire il consenso al trattamento dei dati personali, quando il trattamento sia necessario per finalità di cura dei pazienti (diagnosi, assistenza o terapia sanitaria), purché tali trattamenti siano "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" come previsto dall'art. 9, par. 2, lett. h) e par. 3 del Regolamento UE.

Esercizio dei diritti degli interessati

L'Azienda agevola l'esercizio dei diritti degli interessati previsti dagli artt. 15 e ss. nel rispetto dei principi di semplificazione e trasparenza. 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 utilizzando l'apposito modulo presente nella sezione Privacy del sito internet aziendale.

Accesso alla documentazione sanitaria

I delegati al trattamento curano che siano adottati opportuni accorgimenti per assicurare la comprensibilità dei dati conservati nelle cartelle cliniche o in altra documentazione sanitaria e che siano distinti i dati relativi al paziente da quelli eventualmente riguardanti altri interessati, ivi comprese informazioni relative a nascituri.

Le richieste di presa visione o di rilascio di copia della cartella clinica o in generale di documentazione sanitaria da parte di soggetti diversi dall'interessato possono essere accolte, in tutto o in parte, solo se la richiesta è giustificata dalla documentata necessità:

- di esercitare o difendere un diritto in sede giudiziaria di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale;
- di tutelare, in conformità alla disciplina sull'accesso ai documenti amministrativi, una situazione giuridicamente rilevante di rango pari a quella dell'interessato ovvero consistente 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. 391*quater* 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.

Ricerca e sperimentazioni cliniche

L'Ospedale 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 nel Provvedimento del 5/6/2019 che ha aggiornato, adeguandole al Regolamento UE, le prescrizioni relative al trattamento di dati personali effettuato per scopi di ricerca scientifica di cui alla previgente Autorizzazione Generale n.9/2016; nello specifico agli interessati devono essere comunicate in maniera chiara e comprensibile tutte le informazioni riguardanti le modalità e i fini della ricerca, così che siano in grado di distinguere le attività di ricerca da quelle di tutela della loro salute.

Dati genetici

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 che ha aggiornato, adeguandole al Regolamento UE, le prescrizioni di cui alla previgente n.8/2016 e delle misure di garanzia approvate dall'Autorità Garante in attuazione dell'art. 2-septies del Codice.

Dossier sanitario elettronico aziendale

L'Ospedale ha istituto il proprio Dossier Sanitario Elettronico all'interno dell'applicativo sanitario denominato SIO per la condivisione dei dati sanitari dei propri pazienti; esso contiene le informazioni inerenti allo stato di salute di un individuo, relative ad eventi clinici presenti e trascorsi, volte a documentarne la storia (es.: referti, ricoveri, accessi al pronto soccorso). L'Autorità Garante ha disposto che sia il paziente stesso a scegliere in piena libertà e in virtù del principio di autodeterminazione la costituzione del proprio Dossier, attraverso l'espressione di un consenso raccolto una tantum fatta salva l'eventuale revoca.

Trattamento di dati personali per finalità di trasparenza e pubblicità legale
Gli atti della Azienda soggetti a pubblicazione per finalità di trasparenza e pubblicità legale che riportino dati personali sono pubblicati nel rispetto delle Linee Guida dell'Autorità Garante e delle Circolari aziendali in materia a cui si fa rinvio. Inoltre, nel rispetto del divieto generale di diffusione di dati di natura particolare (cioè relativi a origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale, nonché dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona) e di dati giudiziari, tali dati non possono essere diffusi tramite pubblicazione, essendo invece necessario riportare nel provvedimento da pubblicare il riferimento al fascicolo conservato agli atti del responsabile del procedimento.

Libera Professione
L'Ospedale è Titolare del trattamento dei dati personali nell'ambito della attività libero – professionale erogata dai propri professionisti sanitari sia all'interno delle proprie strutture, sia in spazi sostitutivi.

Sistemi di videosorveglianza
L'installazione di apparecchiature di videosorveglianza è autorizzata dall'Ospedale 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.

Rinvio a norme e provvedimenti aziendali per specifici settori
Si riporta di seguito l'elenco delle tematiche affrontate nel presente Regolamento per le quali si è fatto rinvio a specifici provvedimenti aziendali:

- Disciplinare sull'utilizzo degli strumenti informatici e di comunicazione aziendale
- Procedura aziendale per la gestione del c.d. data breach

Entrata in vigore del Regolamento e forme di pubblicità
Il presente Regolamento entra in vigore dalla data di pubblicazione della determina di approvazione. Il presente Regolamento è redatto allo stato della vigente legislazione ed è soggetto a variazioni o integrazioni a seguito di eventuali successivi interventi normativi o provvedimenti della Autorità Garante per la protezione dei dati personali che dovessero incidere sul suo contenuto. Per tutto quanto non previsto si applica la suddetta normativa di settore. Il Referente Privacy provvede a dare pubblicità al Regolamento tramite la sua pubblicazione nella sezione Privacy del sito Internet e invio a tutti i delegati del trattamento per la relativa diffusione a tutti gli operatori.

Allegati

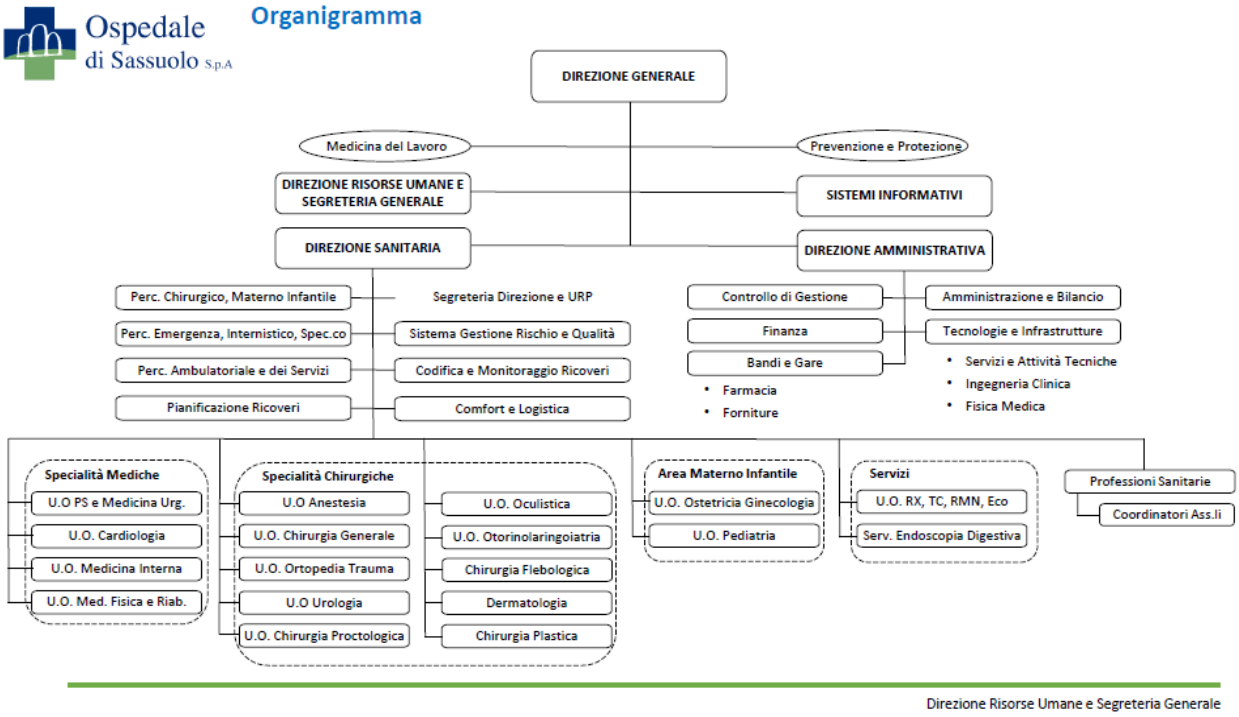
Allegato 1: organigramma

Allegato 2: compiti del delegato al trattamento

Allegato 3: atto di designazione del soggetto autorizzato al trattamento

Allegato 1

ORGANIGRAMMA PRIVACY



Allegato 2

COMPITI E FUNZIONI DEL DELEGATO AL TRATTAMENTO

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, l'Ospedale di Sassuolo S.p.A,, avvalendosi dello strumento della delega, ha attribuito compiti e funzioni proprie del Titolare a figure dirigenziali che di norma corrispondono ai Direttori di Unità Operativa e ai Responsabili di Struttura o di Funzione, nonché al Responsabile delle Professioni Sanitarie. 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, anche per il tramite del Referente Privacy Aziendale e del SIA;
- 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 dall'Ospedale ed assicurare la partecipazione dei propri preposti;
- fornire le informazioni richieste dal Referente Privacy Aziendale, segnalare al medesimo ogni questione rilevante in materia e trasmettere tempestivamente istanze e reclami degli interessati;
- comunicare al Referente Privacy Aziendale 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 della compilazione e del continuo aggiornamento del Registro dei trattamenti aziendale;
- non porre in essere trattamenti di dati diversi e ulteriori senza la preventiva autorizzazione del Titolare del trattamento;
- provvedere, qualora tra le attività istituzionali della struttura vi sia la stipula di contratti o convenzioni con soggetti esterni alla organizzazione che comporti il trattamento di dati personali per conto del Titolare del trattamento, alla contestuale stipula e sottoscrizione del relativo atto di designazione di tali soggetti esterni quali "Responsabili del trattamento" a norma dell'art. 28 del Regolamento UE e delle condizioni ivi indicate;
- comunicare tempestivamente al Referente Privacy Aziendale i potenziali casi di data breach all'interno della propria struttura e collaborare alla istruttoria del caso;
- provvedere, di volta in volta, ad autorizzare al trattamento dei dati personali i singoli operatori per i quali tale autorizzazione non può essere rilasciata contestualmente alla sottoscrizione di un contratto di lavoro/incarico (a titolo non esaustivo: frequentatori volontari, borsisti, lavoratori socialmente utili, stagisti, specializzandi);
- richiedere le autorizzazioni al rilascio delle abilitazioni agli applicativi informatici aziendali per i singoli preposti

Allegato 3

ATTO DI DESIGNAZIONE AL TRATTAMENTO DEI DATI PERSONALI

Ai sensi della normativa vigente in materia di protezione dei dati personali e delle relative disposizioni aziendali, l'Ospedale di Sassuolo S.p.A., Titolare del trattamento dei dati, autorizza la S. V. al trattamento dei dati personali, eventualmente anche contenuti in banche dati informatiche, per quanto necessario allo svolgimento delle mansioni a Lei affidate.

Il trattamento dei dati a cui Lei è autorizzato avviene sotto la diretta autorità del Titolare del trattamento o del Dirigente Responsabile della Unità Operativa o della Struttura/Funzione, alla quale Lei afferisce e che è espressamente delegato dal Titolare a svolgere compiti e funzioni connessi al trattamento di dati personali.

In funzione della presente designazione, Lei è tenuto a:

- trattare i dati in modo lecito e secondo correttezza, attenendosi alle direttive impartite dal Titolare sia con il presente atto, che in seguito, anche per il tramite del dirigente delegato, come sopra individuato;
- trattare i dati esclusivamente per le finalità indicate dal Titolare o dal delegato e unicamente per lo svolgimento delle mansioni a Lei affidate;
- verificare che i dati personali siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti e successivamente trattati;
- trattare i soli dati necessari allo svolgimento delle operazioni da effettuare;
- utilizzare le informazioni e i dati con cui entra in contatto per ragioni di lavoro, comprese categorie particolari di dati personali (cioè relativi a origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale, nonché dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona) e dati giudiziari, esclusivamente per lo svolgimento delle attività istituzionali, con la massima riservatezza sia nei confronti dell'esterno che del personale interno, per tutta la durata dell'incarico ed anche successivamente, al termine di esso;
- verificare l'esattezza ed il grado di aggiornamento dei dati trattati;
- conservare i dati rispettando le misure di sicurezza, tecniche ed organizzative, predisposte dal Titolare del trattamento o dal delegato. In particolare, con riferimento al trattamento di dati personali mediante utilizzo di strumenti elettronici:
  - per le banche dati informatiche, utilizzare sempre il proprio codice di accesso personale evitando di operare su terminali altrui e/o di lasciare aperto il sistema operativo con la propria password inserita in caso di allontanamento anche temporaneo dal posto di lavoro, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento;
  - conservare correttamente i supporti informatici e/o cartacei contenenti i dati personali in modo da evitare che gli stessi siano accessibili a persone non autorizzate;
  - non asportare supporti informatici o cartacei contenenti dati personali di terzi, senza la preventiva autorizzazione del Titolare del trattamento o del delegato;

- segnalare al Titolare del trattamento o al delegato eventuali circostanze che rendano necessario od opportuno l'aggiornamento delle predette misure di sicurezza, al fine di proteggere i dati da trattamenti non autorizzati o illeciti, dal rischio di perdita, di distruzione o di danno accidentale;
- informare immediatamente il Titolare del trattamento o il delegato in caso si constati o si sospetti un incidente di sicurezza, come da procedura aziendale per la gestione del c.d. "data breach";
- astenersi dal comunicare a terzi dati e informazioni senza la preventiva specifica autorizzazione del Titolare del trattamento o del delegato (salvo i casi previsti dalla legge).

Ulteriori istruzioni potranno inoltre esserLe impartite dal Titolare del trattamento o dal delegato, qualora Le siano affidati particolari trattamenti di dati (ad esempio nell'ambito delle sperimentazioni cliniche).

Le istruzioni generali sopra riportate sono integrate dalla procedura aziendale per la gestione del c.d. data breach, di cui Lei è tenuto/a a prendere visione, reperibile sul sito Internet aziendale nella sezione dedicata alla privacy.

Sassuolo, _____

IL DIPENDENTE/COLLABORATORE

Firma _____ (per ricevuta)