OGGETTO: Regolamento recante il sistema di gestione dei dati personali nell'Azienda Usl di Reggio Emilia-IRCCS in applicazione della normativa in materia di protezione dei dati personali - aggiornamento.

IL DIRETTORE GENERALE

Su proposta del Coordinatore degli Staff della Direzione Generale e con contestuale parere favorevole dello stesso in ordine ai contenuti procedurali e formali di legittimità;

Richiamato il Regolamento (UE) Generale sulla Protezione dei dati o GDPR n. 2016/679;

Richiamato il D. Lgs. 196/2003: "Codice in materia di protezione dei dati personali" e le modifiche intervenute alla luce dell'entrata in vigore del D. Lgs. 101/2018;

Preso atto quindi, nell'ambito delle attività di revisione ed adeguamento dell'assetto organizzativo aziendale, in ossequio al principio dell'accountability, delle delibere del Direttore Generale dell'Azienda Usl di Reggio Emilia-IRCCS, i cui contenuti si intendono qui integralmente richiamati e confermati:

- n.16/2018 avente ad oggetto "Costituzione del Comitato Aziendale per la gestione degli aspetti applicativi connessi a quanto previsto dal D.Lgs. 196/2003 - e per quanto innovato - dal Regolamento (UE) Generale sulla Protezione dei dati o GDPR n. 2016/679.", con la quale, alla luce della fusione dell'Azienda Usl di Reggio Emilia e dell'Azienda Ospedaliera Santa Maria Nuova, ai sensi della Legge Regionale E.R. n.9/2017, si determinava l'istituzione di un gruppo di lavoro multidisciplinare vocato ad aggiornare ed uniformare tutte le attività che fin dal secondo semestre 2003 erano state poste in essere in ottemperanza al dettato normativo allora vigente e concernente la protezione dei dati personali, aggiornato nella composizione con deliberazione n. 428 del 16/11/2018;
- n.145/2018, all'oggetto "Determinazioni in merito alla protezione dei dati personali all'interno della Azienda Usl di Reggio Emilia, alla luce del D.Lgs.196/2003 e del Regolamento (UE) generale sulla protezione dei dati n. 2016/679", con la quale si provvedeva a perfezionare e unificare l'esistente schema di regolamento per il trattamento e la tutela dei dati personali all'interno dell'Azienda Usl di Reggio Emilia-IRCCS, ai sensi della Legge Regionale E.R. n.9/2017, avendo tuttavia presente i nuovi principi già inseriti nel regolamento europeo;
- n. 202/2018 all'oggetto "Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali - ricognizione delle prime attività di adeguamento", che effettuava una prima ricognizione delle decisioni prese e delle attività svolte in applicazione della nuova normativa europea, e istituiva l'Ufficio Privacy aziendale;
- n. 228/2018 all'oggetto "Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali - Istituzione ufficio Privacy. Provvedimenti conseguenti", che nominava il responsabile del neoistituito ufficio;
- n. 284 del 25/07/2019 all'oggetto "Regolamento UE 2016/679 - ridefinizione dei profili di responsabilità in tema di protezione dei dati personali e nuove modalità di designazione dei soggetti Responsabili/Delegati e Incaricati/ Autorizzati al trattamento di dati personali", con la quale l'Azienda si dotava di un organizzazione interna articolata sui diversi livelli di responsabilità, che si conferma così come riassunta puntualmente in premessa, ritenuto in tal modo di aver messo in campo un "organigramma" funzionale alla messa a regime dell'auspicata piena realizzazione del dettato normativo ed al fine di strutturare un sistema privacy atto ad infondere nell'organizzazione aziendale la piena consapevolezza dei rischi inerenti i trattamenti, nonché l'affermazione di una cultura della protezione dei dati quale parte integrante dell'intero asset organizzativo, con particolare attenzione alle categorie particolari di dati, tra i quali quelli relativi alla salute; con lo stesso provvedimento l'Azienda provvedeva altresì a designare i referenti dipartimentali e di distretto per la materia, con la finalità di istituire una valida interfaccia e supporto al Responsabile dell'Ufficio Privacy, nella puntuale diffusione delle informazioni e delle determinazioni aziendali concernenti la normativa in vigore sul tema;

Ravvisata oggi la necessità, nell'ottica di piena realizzazione dei principi richiamati dalla citata normativa, di aggiornare il regolamento adottato in fase di prima applicazione della nuova normativa europea, con deliberazione n. 145/2018, anche a seguito dell'intervenuto mutamento organizzativo e del consolidamento del percorso di unificazione aziendale, aggiornandone il testo in ottemperanza a quanto previsto dalla normativa vigente, come da testo allegato alla presente quale parte integrante;

Considerato inoltre che l'aggiornamento del regolamento aziendale in materia di protezione dei dati personali consegue l'obiettivo di cui alla DGR n.977/2019, recante "Linee di programmazione e di finanziamento delle Aziende e degli Enti del Servizio sanitario regionale per l'anno 2019";

Preso atto della condivisione del testo con il DPO ed il Comitato Privacy;

Acquisito il parere favorevole del Direttore Amministrativo e del Direttore Sanitario, espresso ai sensi dell'art. 3 del D. Lgs. n. 502/92 e successive modificazioni ed integrazioni;

DELIBERA

1) Di approvare, per le motivazioni espresse in premessa e qui interamente richiamate, il regolamento, allegato alla presente quale parte integrante, recante l'aggiornamento del documento adottato con deliberazione del Direttore Generale n. 145/2018 e relativo al sistema di gestione dei dati personali nell'Azienda Usl di Reggio Emilia-IRCCS, in applicazione della normativa in materia di protezione dei dati personali;

2) Di provvedere a darne ampia pubblicità mediante pubblicazione sul sito istituzionale nonché sulla intranet aziendale a disposizione degli operatori, nonché alla diffusione tramite la rete dei Referenti Dipartimentali e di Distretto;

3) Di individuare quale responsabile del procedimento ai sensi della legge n. 241/90 la dr.ssa Barbara Gilioli, Responsabile Ufficio Privacy, in Staff alla Direzione Generale;

4) Di trasmettere copia della presente deliberazione al Collegio Sindacale, al Direttore Amministrativo, al Direttore Sanitario, al Direttore delle Attività Socio Sanitarie, ai Distretti Aziendali, al Presidio Ospedaliero, ai Dipartimenti di Sanità Pubblica/Salute Mentale e Dipendenze Patologiche/Farmaceutico/Cure Primarie Aziendale, alle Funzioni di Staff, ai Programmi Aziendali, ai Servizi Amministrativi, ai Servizi Tecnici, al Direttore Scientifico IRCCS, alla Direzione delle Professioni Sanitarie.

Letto, approvato e sottoscritto

Firma apposta digitalmente da:
Il Direttore Generale
Dott. Fausto Nicolini

Sulla presente delibera hanno espresso il parere favorevole:

Firma apposta digitalmente da:
Il Direttore Sanitario
Dott.ssa Cristina Marchesi

Firma apposta digitalmente da:
Il Direttore Amministrativo
Dott.ssa Eva Chiericati

Documento firmato digitalmente e archiviato nel rispetto della normativa vigente.
Il presente documento e' una copia elettronica del documento originale depositato presso gli archivi dell'A.U.S.L. di Reggio Emilia.

DC-28-72-C9-2E-40-55-B3-5E-CE-1A-93-43-CF-6C-3D-73-FC-7E-11

CAdES 1 di 3 del 16/01/2020 18:52:19

Soggetto: CRISTINA MARCHESI

S.N. Certificato: 6D1F B691 906E ABA9

Validità certificato dal 21/12/2017 12:31:57 al 20/12/2023 12:31:57

Rilasciato da Actalis EU Qualified Certificates CA G1, Actalis S.p.A., IT

CAdES 2 di 3 del 18/01/2020 11:05:42

Soggetto: FAUSTO NICOLINI

S.N. Certificato: 423B F4C0 1188 3F70

Validità certificato dal 21/12/2017 12:40:38 al 20/12/2023 12:40:38

Rilasciato da Actalis EU Qualified Certificates CA G1, Actalis S.p.A., IT

CAdES 3 di 3 del 16/01/2020 14:29:11

Soggetto: EVA CHIERICATI

S.N. Certificato: 75D3 A60A E0FA 55CF CCD1 0AAB FF2C 962C

Validità certificato dal 29/10/2019 11:31:37 al 29/10/2025 11:31:37

Rilasciato da Actalis EU Qualified Certificates CA G1, Actalis S.p.A., IT

REGOLAMENTO RECANTE IL SISTEMA DI GESTIONE DEI DATI PERSONALI NELL'AZIENDA USL DI REGGIO EMILIA-IRCCS IN APPLICAZIONE DELLA NORMATIVA IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

ART. 1 PRINCIPI GENERALI E AMBITO DI APPLICAZIONE

L'Azienda USL di Reggio Emilia-IRCCS (di seguito "Azienda" o "Titolare"), 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.
L'Azienda 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 e adotta misure tecniche e organizzative volte a garantire un adeguato livello di sicurezza dei dati, configurando i propri sistemi informativi e i programmi informatici in modo da ridurre al minimo i rischi per i diritti e le libertà degli interessati.
Il presente Regolamento disciplina il sistema di gestione dei dati personali all'interno dell'Azienda USL di Reggio Emilia, nel rispetto della normativa specifica e riguarda tutti i trattamenti dalla stessa effettuati.

ART. 2 NORMATIVA DI RIFERIMENTO

Ai fini del presente Regolamento si intende per:

- "Regolamento UE": il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati);
- "Codice Privacy": il D. Lgs. 30 giugno 2003, n. 196 recante "Codice in materia di protezione dei dati personali" come novellato dal D. Lgs. 10 agosto 2018, n. 101.

Oltre alle norme succitate, a garanzia della conformità dei trattamenti dei dati personali da parte della Azienda alla normativa vigente, sia di natura primaria che di c.d. "*soft law*", trovano inoltre applicazione:

- il vigente Regolamento regionale sui trattamenti dei dati di natura particolare per motivi di interesse pubblico rilevante;
- i Provvedimenti emanati dall'Autorità Garante per la protezione dei dati personali in materie specifiche.

Infine, molti argomenti affrontati nel presente Regolamento sono già stati normati in specifici provvedimenti o circolari aziendali: in questi casi negli articoli interessati ci si limita a fare rinvio a tali atti tempo per tempo vigenti.

ART. 3 TITOLARE DEL TRATTAMENTO

Il Titolare del trattamento è l'Azienda USL di Reggio Emilia- IRCCS che esercita i poteri propri del titolare per mezzo del Legale Rappresentante, il quale può agire d'ufficio o su impulso e/o proposta del Responsabile della Protezione dei Dati (DPO).
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, anche avvalendosi dell'Ufficio Privacy e del Comitato Privacy Aziendale.
Il Titolare provvede a nominare i delegati al trattamento e, al fine di adempiere all'obbligo di cui all'art. 28 del Regolamento UE, a designare quali Responsabili del trattamento – mediante apposito contratto - 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.

ART. 4 REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

L'Azienda 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 l'Ufficio Privacy, a disposizione dell'Autorità Garante per la protezione dei dati personali.

ART. 5 DELEGATI AL TRATTAMENTO: COMPITI E ISTRUZIONI

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'Azienda - con delibera del Direttore Generale N. 284 del 25/07/2018, di revisione del previgente organigramma aziendale - avvalendosi dello strumento della delega, ha attribuito compiti e funzioni proprie del Titolare ai Direttori di Struttura Complessa e ai Responsabili di Struttura Semplice Dipartimentale, nonché a taluni dirigenti/funzionari individuati in virtù delle particolari attività svolte e/o della tipologia dei dati trattati, quali i Responsabili Scientifici di volta in volta individuati nell'ambito di ogni singolo progetto di ricerca/sperimentazione.

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 dell'Ufficio Privacy Aziendale e del Servizio ICT Aziendale;
- 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 dalla Azienda ed assicurare la partecipazione dei propri preposti;
- fornire le informazioni richieste dall'Ufficio Privacy Aziendale, segnalare al medesimo ogni questione rilevante in materia e trasmettere tempestivamente istanze e reclami degli interessati;
- comunicare all'Ufficio 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 all'Ufficio 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.

ART. 6 AUTORIZZATI AL TRATTAMENTO

Con la medesima delibera del Direttore Generale N. 284 del 25/07/2018 è stato definito che tutti i dipendenti/collaboratori che operano sotto la diretta autorità del Titolare siano autorizzati al trattamento dei dati contestualmente alla sottoscrizione del contratto di lavoro o alla accettazione di un incarico lavorativo. Costoro assumono la qualifica di "Autorizzati" al trattamento dei dati e non più di "Incaricati" come previsto dalla previgente normativa. In tal modo non sussiste più l'obbligo in capo al delegato di effettuare la nomina *ad personam* dei propri collaboratori; al fine di garantire continuità con quanto operato in passato, è stata comunque confermata la validità delle nomine ad "Incaricato" del trattamento effettuate in vigenza della precedente normativa e della relativa organizzazione aziendale.

In funzione di tale designazione, i soggetti autorizzati sono tenuti a:
- trattare i dati in modo lecito e secondo correttezza, attendendosi alle direttive impartite dal Titolare sia nell'atto di designazione, sia in seguito, anche per il tramite del dirigente delegato;
- trattare i dati esclusivamente per le finalità indicate dal Titolare o dal delegato e unicamente per lo svolgimento delle mansioni 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 entrino 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 del rapporto lavorativo 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 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 sono inoltre impartite dal Titolare del trattamento o dal delegato, qualora siano affidati

particolari trattamenti di dati (ad esempio nell'ambito delle sperimentazioni cliniche).
Oltre a tali istruzioni generali i soggetti autorizzati al trattamento sono invitati e tenuti a prendere visione dei documenti aziendali, regolamenti e procedure interne vigenti, pubblicati sul sito intranet aziendale, nella sezione dedicata alla Privacy.

ART. 7 RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO)

In applicazione dell'art. 37 del Regolamento UE, che prevede la nomina obbligatoria del Responsabile della Protezione dei Dati (DPO) per tutte le pubbliche amministrazioni, con delibera del Direttore Generale N. 166 del 02/05/2018 l'Azienda ha nominato il proprio DPO, attribuendogli il ruolo e i compiti previsti dagli artt. 38 e 39 del Regolamento UE.

ART. 8 UFFICIO PRIVACY AZIENDALE

L'Ufficio Privacy Aziendale, istituito con deliberazione del Direttore Generale n.202 del 24/05/2018, è inserito nello Staff del Direttore Generale, ed il Responsabile, designato con deliberazione n.228 del 19/06/2018, per la rilevanza strategica della funzione, è invitato permanente al Board di Direzione Strategica. L'Ufficio si occupa di:

- supportare la Direzione Aziendale impostando le procedure per la corretta applicazione della normativa di settore e ne cura gli adempimenti;
- svolgere attività di consulenza e formazione, sia per la Direzione Aziendale, sia nei confronti delle varie articolazioni organizzative, fornendo risposte a quesiti e richieste provenienti dai dipendenti e dagli utenti;
- collaborare con il DPO nella gestione delle segnalazioni di casi di violazione dei dati personali (*data breach*) e delle istanze avanzate dagli interessati al Titolare del trattamento;
- aggiornare e conservare il Registro delle attività di trattamento e il Registro delle violazioni previsti rispettivamente dagli artt. 30 e 33 del Regolamento UE.

ART. 9 COMITATO PRIVACY AZIENDALE E REFERENTI DIPARTIMENTALI

Il Comitato Privacy Aziendale rappresenta un comitato multidisciplinare che discute ed elabora proposte su tematiche privacy di particolare rilevanza e impatto a livello aziendale; garantisce supporto alle attività del Responsabile della Protezione dei Dati e all'Ufficio Privacy, anche ai fini della valutazione dei potenziali casi di violazione dei dati personali, fornisce risposte a istanze che pervengano da strutture aziendali e utenti e promuove azioni di sensibilizzazione verso la materia. Il Comitato Privacy Aziendale è stato istituito con delibera del Direttore Generale N.16 del 18/01/2018.

Con la finalità di istituire una valida interfaccia e supporto al Responsabile dell'Ufficio Privacy, nella puntuale diffusione delle informazioni e delle determinazioni aziendali concernenti la normativa in vigore sul tema, con delibera del Direttore Generale N. 284/2018 si è provveduto a designare referenti dipartimentali e di distretto. Queste figure, in collaborazione con l'Ufficio Privacy, si occupano di diffondere a livello dipartimentale, per singola Unità Operativa, le policy ed i relativi aggiornamenti, fungendo anche da collettori per le eventuali criticità riscontrate nei rispettivi ambiti.

ART. 10 RUOLO DEI SERVIZI ICT E MISURE DI SICUREZZA TECNICHE

Il Servizio di Tecnologie Informatiche e Telematiche (STIT) nell'ambito della rispettiva attività istituzionale, collabora con l'Ufficio Privacy Aziendale ed il Responsabile della Protezione dei Dati e 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;
- in caso di trattamento di dati particolari predisporre misure di minimizzazione e, ove necessario, pseudonimizzazione;
- collaborare alla redazione e all'aggiornamento del Registro delle attività di trattamento;

- 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 Servizio Tecnologie Informatiche e Telematiche, connesse al corretto trattamento dei dati personali, rientrano anche:

- supporto al Servizio di 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) e come "Apparecchiature da Laboratorio" (Dispositivi Medico Diagnostici in Vitro ai sensi della Direttiva 98/79/CE e del Regolamento (UE) 2017/746);
- vigilanza sul rispetto del " Regolamento" interno sull'utilizzo degli strumenti informatici.

Tutti gli operatori di STIT sono autorizzati al trattamento dei dati personali e sono pertanto tenuti al rispetto delle istruzioni indicate all'Art. 5 del presente Regolamento e del Regolamento interno in materia di uso degli strumenti informatici; inoltre, a taluni di essi, espressamente individuati, i Direttori 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.

Il Direttore del Servizio Tecnologie Informatiche e Telematiche attribuisce le funzioni di "Amministratori di Sistema" in conformità al Provvedimento dell'Autorità Garante del 27 Novembre 2008.

ART. 11 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 e sono identificati e registrati i soggetti che vi accedono dopo l'orario di chiusura.
La responsabilità della conservazione e della sicurezza degli archivi amministrativi contenenti dati personali e allocati in strutture aziendali 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 di produzione, 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*.

ART. 12 MISURE DI SICUREZZA ORGANIZZATIVE PER IL RISPETTO DELLA DIGNITÀ' DEGLI INTERESSATI

Nella organizzazione delle prestazioni e dei servizi, l'Azienda 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 comunicazione all'interessato di notizie e informazioni relative al suo stato di salute solamente tramite un medico (designato dall'interessato o dal titolare) o un esercente le professioni sanitarie che abbia un rapporto diretto con l'interessato e sia a ciò stato autorizzato per iscritto;
- la previsione di opportuni accorgimenti volti ad assicurare che, ove necessario, possa essere data correttamente notizia 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.

Per la disamina completa di tutte le misure si fa rinvio alle procedure Aziendali in vigore, pubblicate nell'apposita sezione intranet.

ART. 13 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, diversificata in relazione alle particolarità di taluni trattamenti (ospedali, consultori, sanità pubblica, medicina legale, salute mentale) e distribuita all'interno di tutte le strutture aziendali, mediante affissione nei punti di accesso al pubblico, ben visibili all'utenza, nonché pubblicata sul 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: fornitura di presidi sanitari, ricerca clinica, attività socio-sanitarie integrate.

ART. 14 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 all'Azienda USL di Reggio Emilia-IRCCS, utilizzando l'apposito modulo presente nella sezione Privacy del sito aziendale.

ART. 15 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.
Per quanto concerne la richiesta di copia di cartella clinica o di altra documentazione sanitaria riferita allo stesso richiedente, si rinvia al vigente regolamento aziendale per l'accesso alla documentazione sanitaria.

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.

ART. 16 LIBERA PROFESSIONE

L'Azienda Usl di Reggio Emilia-IRCCS è Titolare del trattamento dei dati personali nell'ambito della attività libero-professionale intramoenia erogata dai propri professionisti sanitari sia all'interno delle proprie strutture, sia in spazi sostitutivi.
Gli aspetti organizzativi, economici e di protezione dei dati sono definiti da apposito regolamento aziendale a cui si fa rinvio.

ART. 17 RICERCA IRCCS, EPIDEMIOLOGICA E SPERIMENTAZIONI CLINICHE

L'Azienda 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 n. 146 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. In tale ambito l'Azienda/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 regolamento aziendale a cui si fa rinvio.

ART. 18 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 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

Garante in attuazione dell'art. 2-septies del Codice.

ART. 19 TRATTAMENTO DI DATI PERSONALI PER FINALITÀ DI TRASPARENZA E PUBBLICITÀ LEGALE

Gli atti dell'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.
In particolare è vietato diffondere tramite pubblicazione 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 dati giudiziari, essendo invece necessario riportare nel provvedimento da pubblicare il riferimento al fascicolo conservato agli atti del responsabile del procedimento.

ART. 20 DOSSIER SANITARIO ELETTRONICO AZIENDALE

L'Azienda ha istituto il proprio Dossier Sanitario Elettronico, c.d. DataWareHouse Clinico (DWH), per la condivisione dei dati sanitari dei pazienti che afferiscono alle sue strutture sanitarie; esso contiene le informazioni inerenti lo stato di salute di un individuo, relative ad eventi clinici presenti e trascorsi (DWH storico), 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.
Stante la complessità di tale strumento e per acquisire le regole di gestione e raccolta del consenso si fa rinvio al relativo regolamento aziendale.

ART. 21 SISTEMI DI VIDEOSORVEGLIANZA

L'installazione di apparecchiature di videosorveglianza è autorizzata dall'Azienda 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.
Per la procedura di installazione degli impianti di videosorveglianza e per le misure di sicurezza da osservare si fa rinvio ad apposito regolamento aziendale.

ART. 22 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:

- Regolamento sull'utilizzo degli strumenti informatici;
- Procedura aziendale per la gestione del c.d. *data breach;*
- Regolamento per il rilascio di documentazione clinica e certificazioni sanitarie;
- Manuale Aziendale relativo alla gestione documentale;
- Regolamento aziendale in materia di Libera Professione;
- Regolamento Aziendale per la ricerca;
- Linee di indirizzo aziendali per la gestione del Dossier Sanitario Elettronico (DWH);
- Regolamento aziendale in materia di videosorveglianza.

ART. 23 ENTRATA IN VIGORE DEL REGOLAMENTO E FORME DI PUBBLICITÀ

Il presente Regolamento entra in vigore dalla data di pubblicazione della deliberazione 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.
L'Ufficio Privacy Aziendale provvede a dare pubblicità al Regolamento tramite la sua pubblicazione nella sezione Privacy dei siti internet e intranet aziendali e invio ai Referenti Dipartimentali e di Distretto e a tutti i delegati del trattamento per la relativa diffusione a tutti gli operatori.