FRONTESPIZIO DELIBERAZIONE

AOO: ASL_BO

REGISTRO: Deliberazione

NUMERO: 0000085

DATA: 15/03/2023 14:40

OGGETTO: AGGIORNAMENTO “LINEE GUIDA PER L’APPLICAZIONE DEL REGOLAMENTO UE 2016/679 E DEL CODICE PRIVACY IN MATERIA DI PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI”

SOTTOSCRITTO DIGITALMENTE DA:

Il presente atto è stato firmato digitalmente da Bordon Paolo in qualità di Direttore Generale
Con il parere favorevole di Roti Lorenzo - Direttore Sanitario
Con il parere favorevole di Ferro Giovanni - Direttore Amministrativo

Su proposta di Gian Carla Pedrazzi - UO Affari Generali e Legali (SC) che esprime parere favorevole in ordine ai contenuti sostanziali, formali e di legittimità del presente atto

CLASSIFICAZIONI:

- [01-08-05]

DESTINATARI:

- Collegio sindacale
- UO Comunicazione (SS)
- Dipartimento Oncologico
- Dipartimento della Rete Medico Specialistica Ospedaliera e Territoriale
- Dipartimento interaziendale ad attivita' integrata di Anatomia Patologica - DIAP
- Dipartimento Cure Primarie
- Dipartimento Materno Infantile
- Dipartimento Interaziendale per la Gestione Integrata del Rischio Infettivo - DIGIRI (IRCCS AOU)
- Dipartimento Medico
- Dipartimento Sanita' Pubblica
- IRCCS Istituto delle Scienze Neurologiche - Direzione Scientifica
- Dipartimento Tecnico-Patrimoniale
- UO Servizio Prevenzione e Protezione (SC)
- UO Anticorruzione e Trasparenza (SC)
- UO Direzione Attivita' Socio-Sanitarie - DASS (SC)
- UO Libera Professione (SC)

L'originale del presente documento, redatto in formato elettronico e firmato digitalmente e' conservato a cura dell'ente produttore secondo normativa vigente.
Ai sensi dell'art. 3bis c4-bis Dlgs 82/2005 e s.m.i., in assenza del domicilio digitale le amministrazioni possono predisporre le comunicazioni ai cittadini come documenti informatici sottoscritti con firma digitale o firma elettronica avanzata ed inviare ai cittadini stessi copia analogica di tali documenti sottoscritti con firma autografa sostituita a mezzo stampa predisposta secondo le disposizioni di cui all'articolo 3 del Dlgs 39/1993.

- UO Affari Generali e Legali (SC)
- UO Ingegneria Clinica (SC)
- UO Governo Clinico, Ricerca, Formazione e Sistema Qualita' (SC)
- UO Governo dei Percorsi di Screening (SC)
- UO Governo dei Percorsi Specialistici (SC)
- UO Sviluppo Organizzativo e Coordinamento Staff (SC)
- UO Sistemi Informativi Aziendali (SC)
- UO Programmazione e Controllo (SC)
- UO Medicina Legale e Risk Management (SC)
- Distretto Savena Idice
- Distretto Pianura Est
- Distretto Pianura Ovest
- Distretto dell'Appennino Bolognese
- Distretto Reno, Lavino e Samoggia
- Dipartimento dell'Integrazione
- Dipartimento della Rete Ospedaliera
- Dipartimento Chirurgie Specialistiche
- Dipartimento Emergenza Interaziendale - DEI
- Dipartimento Chirurgie Generali
- Dipartimento della Riabilitazione
- Dipartimento Salute Mentale - Dipendenze Patologiche
- Dipartimento della Diagnostica e dei Servizi di Supporto
- Dipartimento Farmaceutico Interaziendale - DFI
- Dipartimento Assistenziale, Tecnico e Riabilitativo - DATeR
- Distretto Citta' di Bologna
- UO Committenza e Governo dei Rapporti con il Privato Accreditato (SC)
- DATA PROTECTION OFFICER
- Dipartimento Attivita' Amministrative Territoriali e Ospedaliere - DAATO
- UO Processi Amministrativi Cure Primarie (SC)
- UO Servizi Amministrativi Ospedalieri (SC)
- UO Amministrativa DATeR (SSD)

DOCUMENTI:

File	Firmato digitalmente da	Hash
DELI0000085_2023_delibera_firmata.pdf	Bordon Paolo; Ferro Giovanni; Pedrazzi Gian Carla; Roti Lorenzo	738FE001D6ED01AB7A880392A8D002620 20A2101D3485E8943481EF5D447B889
DELI0000085_2023_Allegato1.pdf:		C35A038506DFE1FE1653970D1914E28F6 FE503459C5839A578EAD2CD03714D0B

L'originale del presente documento, redatto in formato elettronico e firmato digitalmente e' conservato a cura dell'ente produttore secondo normativa vigente.
Ai sensi dell'art. 3bis c4-bis Dlgs 82/2005 e s.m.i., in assenza del domicilio digitale le amministrazioni possono predisporre le comunicazioni ai cittadini come documenti informatici sottoscritti con firma digitale o firma elettronica avanzata ed inviare ai cittadini stessi copia analogica di tali documenti sottoscritti con firma autografa sostituita a mezzo stampa predisposta secondo le disposizioni di cui all'articolo 3 del Dlgs 39/1993.

DELIBERAZIONE

OGGETTO: AGGIORNAMENTO "LINEE GUIDA PER L'APPLICAZIONE DEL REGOLAMENTO UE 2016/679 E DEL CODICE PRIVACY IN MATERIA DI PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI"

IL DIRETTORE GENERALE

Su proposta del Direttore della U.O. Affari Generali e Legali Dr.ssa Gian Carla Pedrazzi, la quale esprime contestuale parere favorevole in ordine ai contenuti sostanziali, formali e di legittimità del presente provvedimento;

Visti:

- il Regolamento (UE) 2016/679 relativo alla Protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati (in seguito "GDPR", General Data Protection Regulation), applicabile in tutti gli Stati membri dell'Unione Europea a partire dal 25 maggio 2018, che nell'affrontare il tema della tutela dei dati personali attraverso un approccio basato principalmente sulla valutazione dei rischi per i diritti e le libertà degli interessati, attribuisce ai Titolari del trattamento il compito di assicurare e di comprovare il rispetto dei principi applicabili al trattamento dei dati personali e di adottare le misure ritenute più idonee ed opportune (c.d. principio di responsabilizzazione o *accountability*);
- il Decreto Legislativo n.101 del 10 agosto 2018 recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio Europeo, in attuazione dell'art.13 della legge di delega europea 2016-2017 (legge 25 ottobre 2017, n.163), che ha introdotto disposizioni per l'adeguamento della normativa nazionale alle disposizioni del GDPR, novellando il Codice Privacy di cui al D.Lgs. n. 196/2003;

Considerato che:

- il richiamato GDPR detta una complessa disciplina di carattere generale in materia di protezione dei dati personali, prevedendo molteplici obblighi ed adempimenti a carico dei soggetti che trattano dati personali, ivi comprese le Aziende Sanitarie, attribuendo al Titolare il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati;
- il " *sistema privacy'* delineato dal GDPR e confermato dal D.Lgs. n. 101/2018 di modifica ed integrazione del D.Lgs. n. 196/2003, implica la necessità di 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 (ivi compresi i dati biometrici e genetici);
- il nuovo approccio comporta il coinvolgimento di tutti i soggetti chiamati a trattare i dati personali all'interno della organizzazione aziendale, con assunzione delle relative responsabilità;

Richiamata la Deliberazione di Giunta Regionale - Emilia Romagna n.919 del 10/4/2018, ad oggetto “Linee di programmazione e di finanziamento delle Aziende e degli enti del Servizio Sanitario regionale per l’anno 2018” la quale ha previsto fra gli obiettivi indicati al punto 4.6 dell’allegato B, oltre alla nomina del Responsabile della Protezione dei Dati (RPD) - Data Protection Officer (DPO) e all’adozione del Registro delle attività di trattamento, la ridefinizione e l’articolazione delle specifiche responsabilità privacy aziendali;

Vista altresì la Deliberazione di Giunta Regionale - Emilia Romagna n.1772 del 24/10/2022 concernente gli Obiettivi di Programmazione Sanitaria Regionale 2022 che, al paragrafo 4,7, individua gli adempimenti relativi alla normativa in materia di protezione dei dati personali tra i quali figura quello relativo all’ aggiornamento delle policy aziendali per il trattamento dei dati attraverso strumenti informatici e per l’ implementazione di nuove applicazioni informatiche (teleconsulto telemedicina, app sanitarie…);

Richiamate le seguenti deliberazioni aziendali:

- n. 31 del 10/2/2020 “Applicazione delle Linee Guida per l’applicazione del Regolamento UE 2016/679 e del Codice privacy in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali”;
- n. 240 del 2/7/2021 *“Presa d’atto della designazione del Responsabile della protezione dei dati dott. ssa Federica Filippini, ai sensi dell’art.37 del Regolamento UE 2016/679”;*
- n. 464 del 2/12/2021 *“Adeguamenti al Regolamento (UE) 2016/679. Definizione dell’organigramma delle responsabilità privacy aziendali e modalità di individuazione dei Referenti Privacy aziendali e dei Soggetti autorizzati al trattamento dei dati personali:aggiornamenti”;*
- n. 400 del 2/11/2022 *“Presa d’atto del documento di definizione dei rapporti tra il data protection officer (DPO) e le funzioni privacy aziendali”;*

Dato atto che il DPO con comunicazione pervenuta via mail del 30/12/2022 ha richiesto l’aggiornamento del documento di cui alla sopra richiamata deliberazione n. 31 del 10/2/2020, predisponendo apposita integrazione del testo relativamente alle informazioni per il trattamento dei dati necessarie per l’erogazione e la gestione delle prestazioni sanitarie per finalità si diagnosi, assistenza, terapia sanitaria o sociale attraverso strumenti informatici (es. telemedicina, teleconsulto ecc);

Ritenuto pertanto di integrare l’art.5 *“Informazioni per il trattamento dei dati personali”* delle Linee Guida per l’applicazione del Regolamento UE 2016/679 e del Codice privacy, relativamente alla gestione delle prestazioni sanitarie per finalità si diagnosi, assistenza, terapia sanitaria o sociale attraverso strumenti informatici (es. telemedicina, teleconsulto ecc);come da documento allegato quale parte integrante alla presente deliberazione (v.p. 5.3);

Considerato altresì che mediante la deliberazione n. 464 del 2/12/2021 era stato temporaneamente sospeso il funzionamento del Gruppo Aziendale Privacy (GAP), in considerazione delle importanti modifiche agli assetti organizzativi aziendali,rinviando a successivo provvedimento la futura composizione di tale organismo in coerenza con i nuovi assetti definiti;

Precisato che la composizione permanente del Gruppo Aziendale Privacy viene ora così determinata:
Direttore UO Affari Generali e Legali o suo delegato (con funzioni di coordinamento);
Direttore UO Tecnologie Informatiche e di Comunicazione o suo delegato;
Direttore UO Anticorruzione Trasparenza o suo delegato;

Dato atto inoltre che, al fine di assicurare la partecipazione al GAP delle diverse macroaree aziendali, in relazione agli ambiti di afferenza delle tematiche privacy di volta in volta da esaminare, la composizione sopra individuata in via permanente debba essere integrata per le specifiche esigenze del caso mediante la partecipazione del:
Direttore Presidio Ospedaliero Unico o suo delegato;
Direttore DAATO o suo delegato;
Direttore DATeR o suo delegato;
Direttore Operativo IRCCS o suo delegato;
Direttore UO Governo Clinico o suo delegato;

Ritenuto di conseguenza di ripristinare il funzionamento del Gruppo Aziendale Privacy nella composizione sopra definita e per le finalità indicate nelle medesime Linee Guida (art.4.4) allegate alla presente deliberazione;

Delibera

per le motivazioni esposte in premessa:

1) di aggiornare le Linee Guida per l'applicazione del Regolamento UE 2016/679 e del Codice privacy in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali,in particolare nella parte relativa alle *"Informazioni per il trattamento dei dati personali"* di cui all'art.5 al fine di ricomprendere anche la gestione delle prestazioni sanitarie per finalità si diagnosi, assistenza, terapia sanitaria o sociale attraverso strumenti informatici (es. telemedicina, teleconsulto ecc); come da documento allegato quale parte integrante alla presente deliberazione;

2) di ripristinare il funzionamento del Gruppo Aziendale Privacy per le finalità indicate nelle suddette Linee Guida (art.4.4) con la seguente composizione permanente:
Direttore UO Affari Generali e Legali o suo delegato (con funzioni di coordinamento);
Direttore UO Tecnologie Informatiche e di Comunicazione o suo delegato;
Direttore UO Anticorruzione Trasparenza o suo delegato;

3) Di precisare che la suddetta composizione permanente del GAP sarà di volta in volta integrata, in relazione alle specifiche tematiche privacy da trattare, mediante la partecipazione del:
Direttore Presidio Ospedaliero Unico o suo delegato;
Direttore DAATO o suo delegato;
Direttore DATeR o suo delegato;
Direttore Operativo IRCCS o suo delegato;

Direttore UO Governo Clinico o suo delegato;

4) di precisare che il presente provvedimento verrà pubblicato alla pagina privacy policy del sito internet dell'Azienda USL;

5) di trasmettere copia del presente provvedimento al Responsabile Protezione Dati (DPO) ed a tutti i Dipartimenti, Distretti e Strutture di Staff.

Responsabile del procedimento ai sensi della L. 241/90:
Rosa Preiti

Linee Guida per l’applicazione del Regolamento (UE) 2016/679 (GDPR) e del Codice Privacy in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali

SOMMARIO

PREMESSE

Le presenti Linee Guida disciplinano il sistema di gestione dei dati personali all'interno dell'Azienda USL di Bologna, nel rispetto della normativa specifica, e riguardano tutti i trattamenti effettuati dalla stessa o per suo conto.

Le presenti Linee Guida si richiamano al 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 (c.d. regolamento generale sulla protezione dei dati), e al Decreto Legislativo 30 giugno 2003 n.196, recante il "Codice in materia di protezione dei dati personali", così come modificato dal Decreto Legislativo n.101 del 10 agosto 2018, recante "Disposizioni per l'adeguamento della normativa nazionale al 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".

A garanzia della conformità alla normativa vigente, ai trattamenti dei dati personali effettuati dall'Azienda si applicano:

- 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.

Le presenti linee guida contengono rinvii e richiami ad atti contenenti specifiche disposizioni, istruzioni, indicazioni e procedure. Per tutto quanto non espressamente riportato, si rinvia a tutti gli atti e documenti rinvenibili alla sezione "privacy policy" del sito web istituzionale, consultabili al link: https://www.ausl.bologna.it/privacy

PARTE PRIMA
DISPOSIZIONI GENERALI

ART. 1 PRINCIPI GENERALI

Il trattamento dei dati personali, nell'ambito di ogni articolazione organizzativa dell'Azienda USL di Bologna, viene effettuato garantendo a chiunque il rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali. Al trattamento dei dati personali si applicano i principi di cui all'art.5 del Regolamento (UE) 2016/679 (liceità, correttezza e trasparenza; limitazione delle finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza; responsabilizzazione).

Il trattamento dei dati personali viene disciplinato dall'Azienda USL di Bologna assicurando un elevato livello di tutela dei diritti e delle libertà di cui sopra, nel rispetto dei principi di semplificazione, armonizzazione ed efficacia delle modalità previste per il loro esercizio da parte degli interessati e per l'adempimento degli obblighi da parte del Titolare del trattamento.

Le presenti linee guida si applicano al trattamento dei dati personali, anche se detenuti all'estero, effettuato dall'Azienda USL di Bologna.

ART. 2 OGGETTO E FINALITÀ

Le presenti linee guida rappresentano lo strumento con il quale l'Azienda Unità Sanitaria Locale di Bologna specifica e fissa i compiti e le regole alle quali devono attenersi i Referenti Privacy, tutti i soggetti autorizzati al trattamento dei dati personali ed i responsabili di trattamento designati, fermo restando quanto disposto dal Regolamento UE, dal Codice e dalle altre disposizioni in materia di protezione dei dati.

ART. 3 DEFINIZIONI

Ai fini dell'individuazione del significato dei termini utilizzati nel presente atto si applicano le definizioni di cui alla normativa vigente di seguito elencate:

- «dato personale»: qualsiasi informazione riguardante una persona fisica, identificata o identificabile («interessato»), direttamente o indirettamente, come il nome di una persona fisica, un numero di identificazione, dati relativi all'ubicazione, a recapiti telefonici, ad un identificativo on-line, e-mail o a uno

o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

- «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;
- «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
- «profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
- «pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
- «archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
- «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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il Titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
- «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;
- «amministratore di sistema»: figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP (Enterprise Resource Planning) utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali;
- «destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
- «interessato»: la persona fisica cui si riferiscono i dati personali;
- «terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il Titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del Titolare o del responsabile;
- «consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesti il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, affinché i dati personali che lo riguardano siano oggetto di trattamento;
- «violazione dei dati personali» o «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.
- rientrano nella categoria dei «dati particolari»:
  - «dati genetici»: dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona

fisica in questione;
  - «dati biometrici»: dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o Confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
  - «dati relativi alla salute»: dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

- «comunicazione»: il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del Titolare nel territorio dello Stato, dal responsabile, dagli autorizzati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- «dato anonimo»: dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
- «diffusione»: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- «Data Protection Officer» (DPO) o «Responsabile della Protezione dei Dati» (RPD): figura prevista dal Regolamento Europeo, quale supporto del Titolare, con la finalità di facilitare l'attuazione della normativa (artt.37, 38 e 39 del Regolamento UE);
- «Gruppo Aziendale Privacy» (GAP): gruppo di professionisti che, in attuazione dei principi di informazione e sensibilizzazione richiamati dal Regolamento UE, ha il compito di assicurare un presidio aziendale per quel che concerne gli adempimenti organizzativi e procedurali derivanti dalle nuove disposizioni normative in materia di protezione dei dati personali;
- **«**Responsabile del trattamento**»** (ex «Responsabile esterno»): persona fisica o giuridica, autorità pubblica, servizio o altro organismo esterno rispetto all'Azienda USL di Bologna, che, in virtù di un atto di designazione, tratta dati personali per conto del Titolare del trattamento;
- «Referente Privacy» (ex «Responsabile interno di trattamento»): soggetto qualificato, interno all'Azienda, a cui il Titolare assegna compiti e funzioni connessi al trattamento di dati personali;
- «Soggetto autorizzato al trattamento» (ex «incaricato di trattamento»): la persona fisica autorizzata dal Titolare o dal Referente Privacy a compiere operazioni di trattamento;
- «Funzioni Aziendali Privacy»: funzioni nell'ambito dell'UO Affari Generali e Legali di supporto al Titolare che, interagendo con tutte le strutture/articolazioni organizzative trasversali/di supporto, con i Dipartimenti ad Attività Integrata e con le strutture ad essi afferenti, hanno la finalità di garantire e coordinare le attività aziendali correlate alla normativa in materia di protezione dei dati personali, anche interagendo con il Data Protection Officer (DPO);
- «Garante per la protezione dei dati personali»: Autorità indipendente, con sede a Roma, istituita dalla c.d. Legge sulla privacy (Legge 31 dicembre 1996, n.675) per assicurare la tutela dei diritti e delle libertà fondamentali ed il rispetto della dignità nel trattamento dei dati personali. É un organo collegiale, composto da quattro membri eletti dal Parlamento, i quali rimangono in carica per un mandato di sette anni non rinnovabile (www.garanteprivacy.it);
- «Informazioni»: requisito fondamentale di legittimità del trattamento dei dati personali. É lo strumento che rende esplicita e trasparente la gestione dei dati di carattere personale e/o particolare degli interessati. Attraverso le informazioni l'interessato acquisisce ogni necessaria conoscenza circa l'utilizzo dei propri dati personali, a tutela del corretto trattamento del dato;
- «Misure adeguate»: complesso di misure tecniche, informatiche, organizzative, logistiche e procedurali che configurano un livello di sicurezza, adeguato, in relazione ai rischi previsti nell'articolo 32 Regolamento UE;
- **«**Registro delle attività di trattamento**»**: ai sensi dell'art.30 del Regolamento UE 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 effettuati nello svolgimento della propria attività istituzionale. Il Registro è depositato presso l'Azienda USL di Bologna a disposizione, su richiesta, dell'Autorità Garante per la protezione dei dati personali;
- «GDPR» o «RGPD»: General Data Protection Regulation o Regolamento per la Protezione dei Dati Personali, di cui al Regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, di seguito, in breve, *Regolamento UE;*
- «Codice privacy»: decreto legislativo 30 giugno 2003, n.196, recante il "Codice in materia di protezione

dei dati personali" come integrato dalle modifiche introdotte dal decreto legislativo 10 agosto 2018, n.101, recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679. Di seguito, per brevità, *Codice*;

- *«Privacy policy»:* sezione del sito web istituzionale ove è possibile consultare ogni indicazione utile, per la protezione dei dati personali, fornita dal Titolare di trattamento. https://www.ausl.bologna.it/privacy

PARTE SECONDA
RUOLI E RESPONSABILITÀ

ART. 4 ORGANIGRAMMA DELLE RESPONSABILITÀ PRIVACY AZIENDALI

4.1 TITOLARE DEL TRATTAMENTO

Il Titolare del trattamento dei dati è l'Azienda USL di Bologna, persona giuridica di diritto pubblico, istituita con Legge Regionale n. 21 del 20 ottobre 2003, che esercita i poteri propri del Titolare del trattamento per mezzo del Legale Rappresentante che può agire d'ufficio o su impulso e/o proposta del Responsabile della Protezione dei Dati (Data Protection Officer - DPO).

Il Titolare del trattamento, 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, avvalendosi della collaborazione del DPO, dei Referenti Privacy, delle Funzioni Aziendali Privacy, della UO Tecnologie Informatiche e di Comunicazione e del Gruppo Aziendale Privacy.

Il Titolare provvede a nominare i Referenti Privacy e, ai sensi dell'art. 28 del Regolamento UE, a designare quali Responsabili del trattamento, mediante apposito atto, 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, solo se presentano garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate e rispondenti ai requisiti del Regolamento UE garantendo la tutela dei diritti dell'interessato.

4.2 DATA PROTECTION OFFICER (DPO)

È una figura esterna all'Azienda USL di Bologna, che svolge le seguenti attività:

> informa e fornisce consulenza all'Azienda USL di Bologna in ordine agli obblighi derivanti dal Regolamento, nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati. Per il tramite dei Referenti Privacy assicura attività di informazione/consulenza ai Referenti Privacy Aziendali nonché ai dipendenti e collaboratori che, in qualità di autorizzati al trattamento, eseguono operazioni di trattamento dati;
> vigila sulla corretta osservanza della normativa in materia di protezione dei dati personali nonché delle policy aziendali, comprese l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti, coordinando il gruppo dei referenti/responsabili privacy individuati dalle aziende dell'area metropolitana;
> fornisce, se richiesti, pareri anche scritti in merito alla valutazione d'impatto sulla protezione dei dati e ne sorveglia lo svolgimento;
> coopera 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), effettua eventuali consultazioni e ne cura in generale i rapporti;
> fornisce supporto alla tenuta del Registro delle attività di trattamento;
> interloquisce con gli altri DPO delle Aziende sanitarie regionali e/o con il DPO della Regione Emilia-Romagna in relazione a progetti ed iniziative di valenza regionale/metropolitana (ad es. FSE, ARA, GRU, GAAC);
> promuove iniziative congiunte tra le Aziende/Enti dell'area di metropolitana affinché l'applicazione della normativa in materia di protezione dei dati personali, nonché delle policy aziendali, sia sviluppata secondo linee applicative omogenee e coerenti nelle singole Aziende/Enti;
> favorisce il coordinamento dei DPO delle altre aziende sanitarie regionali relativamente alle tematiche precedentemente presidiate dal Tavolo Privacy Regionale, come da richiesta della Regione Emilia-Romagna di cui alla nota PG/2018/0482475 del 5 luglio 2018.

4.3 REFERENTI PRIVACY PER IL TRATTAMENTO DEI DATI

L'Azienda USL di Bologna, con la Deliberazione n.11 del 14.01.2019 "*Adeguamenti al Regolamento (UE) 2016/679. Definizione dell'organigramma delle responsabilità privacy aziendali e modalità di individuazione*

dei Referenti Privacy aziendali e dei soggetti autorizzati al trattamento dei dati personali", aggiornata con deliberazione n. 464 del 2/12/2021,ha individuato quali “Referenti Privacy" i Direttori di Unità Operativa Complessa (SC), i Dirigenti Responsabili di Unità Operativa Semplice Dipartimentale (UOSD) e i Direttori di Programmi Gestionali.

La qualifica di Referente Privacy si estende ai dirigenti che, in caso di vacanza del ruolo del Direttore o del Responsabile, assumano la relativa responsabilità ad interim.

Il Direttore Generale si riserva la facoltà di designare ulteriori Referenti Privacy in virtù delle particolarità organizzative e funzionali delle attività di competenza e/o della tipologia dei dati trattati.

La designazione di Referente Privacy avviene all’atto del conferimento dell’incarico dirigenziale.

Nel rispetto delle funzioni e dei poteri attribuiti dal Direttore Generale, i Referenti Privacy, rispetto ai trattamenti di dati svolti nell’ambito della propria sfera di competenze, provvedono a:

1. osservare e fare osservare:
   a) le policy aziendali in materia di protezione, di finalità, di modalità di trattamento dei dati, fornite dal Titolare del trattamento, anche per il tramite delle Funzioni Aziendali Privacy, del Gruppo Aziendale Privacy (GAP) e della UO Tecnologie Informatiche e di Comunicazione (es. Regolamento aziendale sull’utilizzo delle risorse informatiche, Linee di indirizzo per la gestione del Dossier Sanitario Elettronico, Procedura per la gestione della violazione dei dati personali o data breach, ecc.);
   b) le istruzioni di carattere generale impartite dal Titolare a tutti i soggetti autorizzati al trattamento dei dati personali (di cui all’allegato 2 della Deliberazione n.11 del 14.01.2019 e s.m.i.);
   c) eventuali ulteriori specifiche istruzioni impartite dal Titolare o dallo stesso Referente Privacy, in relazione agli specifici ambiti di competenza, anche per gruppi omogenei di funzioni;
   d) procedure e linee guida aziendali per la corretta gestione dei dati, assicurando che i soggetti interessati (ad es. pazienti, dipendenti, fornitori, ecc.) ricevano le informazioni relative al trattamento dei dati personali di cui agli artt.13 e 14 del Regolamento UE.

2. Designare i soggetti autorizzati al trattamento dei dati personali. Per coloro ai quali l’autorizzazione non può essere rilasciata contestualmente alla sottoscrizione del contratto di lavoro/incarico (a titolo esemplificativo e non esaustivo: frequentatori volontari, lavoratori socialmente utili, etc.), attraverso la predisposizione dell’apposito format di cui l’allegato 3 della già citata Deliberazione aziendale n.11 del 14.01.2019 e s.m.i
3. Vigilare sulla conformità dell’operato dei soggetti autorizzati, ad essi afferenti, alle istruzioni e alle direttive di cui sopra, verificando periodicamente lo stato di adeguamento alla normativa in oggetto;
4. Verificare che i dati oggetto di trattamento siano esatti, aggiornati, indispensabili, pertinenti e non eccedenti rispetto alle finalità per cui vengono trattati;
5. Attenersi alle indicazioni di sicurezza dettate dal Titolare del trattamento e, 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;
6. Partecipare ai momenti formativi organizzati dal DPO e dall’Azienda USL di Bologna ed assicurare la partecipazione dei soggetti autorizzati;
7. Fornire le informazioni richieste dalle Funzioni Aziendali Privacy e dal Gruppo Aziendale Privacy (GAP), segnalare ogni questione rilevante in materia e trasmettere tempestivamente istanze e reclami degli interessati, da far pervenire al DPO;
8. Comunicare alle Funzioni Aziendali Privacy e al Gruppo Aziendale Privacy (GAP) 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 delle attività di trattamento aziendale;
9. Collaborare con le Funzioni Aziendali Privacy e con il Gruppo Aziendale Privacy (GAP) per la predisposizione del documento della valutazione di impatto sulla protezione dei dati, qualora ne ricorrano i presupposti in base all’art.35 del Regolamento UE;
10. Astenersi dal porre in essere trattamenti di dati personali diversi e ulteriori senza la preventiva autorizzazione del Titolare del trattamento;
11. Provvedere qualora tra le attività istituzionale della struttura vi sia la stipula di contratti/convenzioni/accordi con soggetti esterni, alla organizzazione che comportano il trattamento di dati personali per conto del Titolare alla contestuale stipula o predisposizione del relativo atto di designazione di tali soggetti esterni, quali “responsabili del trattamento” a norma dell'art.28 del

Regolamento UE e alla trasmissione di copia di tale atto di designazione e della relativa accettazione della nomina alle Funzioni Aziendali Privacy, anche ai fini dell'aggiornamento del Registro delle attività di trattamento dei dati aziendale;

12. Comunicare tempestivamente alle Funzioni Aziendali Privacy e al Gruppo Aziendale Privacy (GAP) i potenziali casi di data breach verificatisi all'interno della propria struttura e collaborare alla istruttoria del caso, al fine di sottoporre al DPO ogni utile ed opportuna determinazione in merito.

4.4 GRUPPO AZIENDALE PRIVACY (GAP)

Il Gruppo Aziendale Privacy (GAP) ha il mandato di assicurare un presidio aziendale per quanto concerne gli adempimenti organizzativi e procedurali derivanti dalle disposizioni normative in materia di protezione dei dati personali ed è così composto :

Membri permanenti:
Direttore UO Affari Generali e Legali o suo delegato (con funzioni di coordinamento);
Direttore UO Tecnologie Informatiche e di Comunicazione o suo delegato;
Direttore UO Anticorruzione Trasparenza o suo delegato;

Al fine di assicurare la partecipazione al GAP delle diverse macroaree aziendali, in relazione agli ambiti di afferenza delle tematiche privacy di volta in volta da esaminare, la composizione del GAP è integrata mediante la partecipazione del:

Direttore Presidio Ospedaliero Unico o suo delegato;
Direttore DAATO o suo delegato;
Direttore DATeR o suo delegato;
Direttore Operativo IRCCS o suo delegato;
Direttore UO Governo Clinico o suo delegato;

Il GAP fornisce inoltre supporto ai Referenti Privacy nelle attività di:

a) adozione di misure adeguate ed efficaci per la tutela della riservatezza, integrità e disponibilità del patrimonio informativo;
b) aggiornamento del Registro delle attività di trattamento di dati personali effettuate dalle strutture di appartenenza dei componenti e nell'eventuale valutazione di impatto, in collaborazione con la UO Tecnologie Informatiche e di Comunicazione;
c) espletamento di verifiche di sicurezza svolte dalla UO Tecnologie Informatiche e di Comunicazione e/o dal DPO;
d) coordinamento delle richieste di parere da sottoporre al DPO formulate dai singoli Referenti Privacy;
e) valutazione del rischio, a seguito dell'istruttoria effettuata su segnalazione di violazione, per fornire ogni utile elemento al Titolare del trattamento.

4.5 RUOLO DEL DIRETTORE DELLA UO TECNOLOGIE INFORMATICHE E DI COMUNICAZIONE

Al Direttore UO Tecnologie Informatiche e di Comunicazione, Referente Privacy, spettano i seguenti compiti:

- sovrintendere alle risorse del sistema informatico centralizzato (software dipartimentali e trasversali) e consentirne l'utilizzazione a tutti i Referenti e soggetti autorizzati, mediante l'adozione delle misure di sicurezza tecniche di cui all'art.32 del Regolamento UE;
- garantire la gestione e manutenzione degli strumenti elettronici aziendali;
- garantire la protezione dei dispositivi e dei programmi contro il rischio di intrusione e dell'azione di programmi di cui all'art.615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale;
- garantire gli aggiornamenti periodici, almeno con cadenza annuale, dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici ed a correggerne difetti. In caso di trattamento di dati particolari l'aggiornamento deve essere svolto semestralmente;
- impartire istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno quotidiana e, comunque, che garantiscano tempestivamente il ripristino, la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- adottare idonee misure che assicurino l'integrità e la disponibilità dei dati;
- adottare idonee misure che assicurino il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni;

- in caso di trattamento di dati particolari, predisporre misure di pseudonimizzazione e cifratura dei dati personali, anche garantendo il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati;
- redigere il Registro delle attività del trattamento, eventualmente previa consultazione con il Responsabile della Protezione dei Dati, anche dando indicazioni ai Referenti per la trasmissione delle informazioni necessarie per l'aggiornamento del Registro stesso;
- procedere, laddove ritenuto necessario e/o opportuno alla valutazione di impatto di cui all'articolo 35 del Regolamento UE, avvalendosi della consulenza del DPO, avvisando il Titolare laddove derivi la necessità di procedere alla consultazione preventiva di cui all'articolo 36 del Regolamento UE;
- implementare ogni misura finalizzata al rispetto del disciplinare interno sull'uso dei sistemi informativi.

Tenuto conto del fatto che l'accesso ai dati e alle procedure aziendali è consentito, per necessità di operatività e sicurezza dei sistemi, ai soggetti autorizzati della UO Tecnologie Informatiche e di Comunicazione cui sono attribuite le caratteristiche di super-utente, il Direttore della UO procede all'individuazione del preposto all'intervento su sistemi e procedure aziendali in assenza dei soggetti autorizzati al trattamento, se pur nel rispetto del disciplinare interno in materia di uso dei sistemi informativi.

4.6 SOGGETTO AUTORIZZATO AL TRATTAMENTO DEI DATI PERSONALI

Ai fini dell'autorizzazione al trattamento, prevista dall'art. 2-quaterdecies del D.lgs. n.196/2003 e s.m.i. come indicato dalla Deliberazione n.11 del 14.01.2019 e s.m.i., per "personale autorizzato al trattamento dei dati" (già «personale incaricato di trattamento dati») s'intende, in via generale, tutto il personale dipendente dell'Azienda USL di Bologna, 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, alla data di adozione della citata deliberazione , 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 al Servizio Unico Metropolitano Amministrazione Giuridica 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 trasferimento e/o mutamento di mansioni. Contestualmente vengono fornite le istruzioni operative di carattere generale di cui all'allegato 3 della Deliberazione n.11 del 14.01.2019 e s.m.i.

Per i tirocinanti, frequentatori, specializzandi, medici in formazione specialistica, l'atto autorizzativo viene rilasciato dalla UO Sviluppo Organizzativo, Professionale e Formazione, che fornisce contestualmente le istruzioni operative di carattere generale di cui all'allegato 2 della Deliberazione n.11 del 14.01.2019 e s.m.i.;

Per il personale in convenzione spetta al Dipartimento delle Cure Primarie provvedere alla nomina di soggetto autorizzato all'atto della sottoscrizione della convenzione.

I soggetti autorizzati al trattamento sono tenuti a partecipare agli incontri ed alle iniziative di formazione organizzate periodicamente e/o indicate dal Titolare, dai Referenti Privacy e dal Responsabile della Protezione dei Dati (DPO) .

4.7 RESPONSABILE DEL TRATTAMENTO

Il Responsabile del trattamento» (ex «Responsabile esterno») è la persona fisica o giuridica, autorità pubblica, servizio o altro organismo esterno rispetto all'Azienda USL di Bologna, che, in virtù di rapporti contrattuali o convenzionali, previa designazione, tratta dati personali per conto del Titolare del trattamento.
L'atto di designazione viene predisposto secondo schema tipo, redatto secondo le disposizioni del Regolamento UE 2016/679, adottato dal Titolare del Trattamento e pubblicato sul sito web aziendale nell'apposita sezione Policy Privacy.

Nel rispetto delle istruzioni operative impartite dal Titolare, spetta al Direttore/dirigente responsabile del procedimento relativo al rapporto contrattuale o convenzionale con soggetti esterni provvedere alla designazione di tali soggetti contestualmente alla sottoscrizione del contratto/accordo/convenzione, quali

“responsabili del trattamento” a norma dell'art.28 del Regolamento UE.

Alla UO Affari Generali e Legali-Funzioni Aziendali Privacy deve pervenire evidenza di tale designazione, anche ai fini dell’aggiornamento del Registro delle attività di trattamento .

PARTE TERZA
INFORMAZIONI SUL TRATTAMENTO DEI DATI PERSONALI

ART. 5 INFORMAZIONI PER IL TRATTAMENTO DI DATI PERSONALI

I Referenti Privacy 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 dalle Funzioni Aziendali Privacy nel rispetto delle indicazioni fornite dal Titolare del trattamento e/o dal Responsabile della Protezione dei Dati.
Le Funzioni Aziendali Privacy hanno cura che le informazioni sul trattamento dei dati personali siano rese note anche mediante pubblicazione nel sito internet aziendale, nell’apposita sezione Privacy Policy al link: https://www.ausl.bologna.it/privacy

5.1 INFORMAZIONI PER I TRATTAMENTI DI DATI PERSONALI NECESSARI A SOLI FINI AMMINISTRATIVI

L’Azienda USL di Bologna tratta i dati personali per fini amministrativi nel rispetto di quanto previsto dall’articolo 6, par. 2, lettera e) del Regolamento UE, ovvero solo se necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investita, e per le finalità di cui dell’articolo 9, par.2, lettera g) del medesimo Regolamento UE, ovvero quando il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri.

5.2 INFORMAZIONI PER I TRATTAMENTI DI DATI PERSONALI, NECESSARI PER L’EROGAZIONE E LA GESTIONE DELLE PRESTAZIONI SANITARIE, PER FINALITÀ DI DIAGNOSI, ASSISTENZA, TERAPIA SANITARIA O SOCIALE

L’Azienda USL di Bologna 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 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 l’Azienda USL di Bologna (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.

Ulteriori specifici trattamenti di dati relativi alla salute sono effettuati mettendo a disposizione dell’interessato informazioni integrative e richiedendo, se previsto, uno specifico ed esplicito consenso.

In particolare, a condizione che l’interessato abbia espresso il proprio specifico consenso, possono essere effettuati trattamenti quali:

- la costituzione e l’alimentazione del Dossier Sanitario Elettronico e del Fascicolo Sanitario Elettronico;
- l’implementazione dei sistemi di sorveglianza/registri di patologia;
- i trattamenti a scopi di ricerca scientifica anche nell’ambito delle sperimentazioni cliniche (tranne alcuni

casi specifici previsti dalla legge);
- i trattamenti di dati genetici e/o biometrici;
- la comunicazione di dati al medico di fiducia o ad altri soggetti (es. Rete SOLE);
- i servizi di refertazione on-line.

5.3 INFORMAZIONI PER I TRATTAMENTI DI DATI PERSONALI,PER L'EROGAZIONE E LA GESTIONE DELLE PRESTAZIONI SANITARIE,PER FINALITA' DI DIAGNOSI, ASSISTENZA, TERAPIA SANITARIA O SOCIALE ATTRAVERSO STRUMENTI INFORMATICI (TELEMEDICINA, TELECONSULTO ECC…)

L'Azienda USL di Bologna promuove e attua la Telemedicina quale modalità attraverso la quale erogare a distanza prestazioni sanitarie di routine svolte in presenza come la visita, il consulto, il monitoraggio di parametri e l'assistenza.

Attraverso tale modalità si erogano prestazioni di prevenzione, diagnosi, cura e riabilitazione inserite nei LEA e quindi riconosciute nel nomenclatore tariffario come prestazioni erogate in via telematica, in particolare per la presa in carico domiciliare secondo PDTA delle patologie croniche.

La telemedicina non sostituisce la medicina tradizionale, ma la affianca e la integra con nuovi canali di comunicazione e tecnologie innovative, con l'obiettivo di migliorare l'assistenza sanitaria e aiutare i cittadini ad accedere ed ottenere le migliori cure possibili.

Tale modalità può interessare tanto la pratica clinica diagnostica, assistenziale e riabilitativa quanto l'ambito dell'innovazione, ricerca scientifica e sviluppo.

L'Azienda USL esegue il trattamento dei dati personali effettuato tramite gli applicativi che consentono la televisita, nella piana osservanza delle normative europee e nazionali e adottando misure tecniche ed organizzative adeguate quali:
- la progettazione del trattamento secondo una analisi di privacy by design e by default (art. 25 GDPR);
- l'analisi del rischio e la valutazione di impatto (art. 35 GDPR);
- l'aggiornamento del registro dei trattamenti (art. 30 GDPR).

5.4 INFORMAZIONI PER I TRATTAMENTI DI DATI PERSONALI PER FINALITÀ DI RICERCA MEDICO SCIENTIFICA, BIOMEDICA ED EPIDEMIOLOGICA

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 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. A tal fine, in particolare, il modulo contenente le predette informazioni, così come il modulo da sottoporre al paziente per la prestazione del consenso al trattamento dei suoi dati per finalità di ricerca e sperimentazione, laddove necessario, deve essere predisposto separatamente da quello predisposto per la partecipazione alla ricerca.

Precise indicazioni per la predisposizione delle informazioni sul trattamento dei dati personali per attività di ricerca, nei due distinti casi in cui oggetto del trattamento siano dati *personali e particolari* oppure *personali, particolari e genetici*, sono pubblicate e raggiungibili dalla sezione *privacy policy* del sito web istituzionale: https://www.ausl.bologna.it/privacy

5.5 INFORMAZIONI PER I TRATTAMENTI DI DATI PERSONALI NELL'AMBITO DEL RAPPORTO CONTRATTUALE, LAVORATIVO, PROFESSIONALE, AUTONOMO E CONVENZIONALE

L'Azienda USL di Bologna tratta i dati per i fini di cui all'articolo 6, par.2, lettera b) del Regolamento UE, ovvero quando 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, nonché per i fini di cui all'art.6, par. 2, lettera b) del medesimo Regolamento UE, ovvero quando il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del Titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale.

I Referenti Privacy sono tenuti a porre in essere ogni atto necessario per fornire agli interessati le informazioni di cui agli articoli 13 e 14 del Regolamento UE, nel rispetto delle indicazioni fornite dal Titolare.

In ogni caso le predette informazioni dovranno essere inserite nei relativi atti contrattuali e, laddove il rapporto sia soggetto a procedure concorsuali, le predette informazioni dovranno essere necessariamente contenute nei bandi di concorso, di gara, nelle lettere di invito e/o avvisi pubblici.

Le informazioni sulla protezione e il trattamento dei dati personali rivolte a dipendenti, terzi non dipendenti (liberi professionisti, consulenti, docenti, convenzionati, ecc.) e fornitori sono comunque pubblicate all'interno del sistema di Gestione delle Risorse Umane - GRU e pubblicate nell'apposita sezione *privacy policy* del sito web istituzionale: https://www.ausl.bologna.it/privacy

5.6 ALTRE INFORMAZIONI SUL TRATTAMENTO DI DATI PERSONALI

Le informazioni sul trattamento dei dati personali adottate dall'Azienda USL di Bologna sono consultabili alla pagina:
https://www.ausl.bologna.it/privacy/informative-sul-trattamento-dei-dati-personali-1/informative-sul-trattamento-dei-dati-personali

Spetta ai Referenti Privacy, ognuno per lo specifico ambito di competenza, diffondere ed applicare le informazioni di cui agli artt.13 e 14 del Regolamento UE definite dal Titolare del trattamento.

ART. 6 TRATTAMENTO DEI DATI NEGLI ATTI SOGGETTI A PUBBLICAZIONE

Gli atti dell'Azienda AUSL di Bologna soggetti a pubblicazione contenenti dati particolari di cui agli articoli 9 e 10 del Regolamento UE, i provvedimenti disciplinari e gli atti concernenti i minori, non possono essere pubblicati in forma identificativa diretta e indiretta.

Sarà cura dei Referenti Privacy, sentito il Direttore della UO Tecnologie informatiche e Comunicazione, valutare le opportune modalità di pseudoanonimizzazione o anonimizzazione, previa consultazione del Responsabile per la protezione dei dati, assicurando in ogni caso al diretto interessato la possibilità di potersi identificare.

PARTE QUARTA
ALTRI TRATTAMENTI DI DATI PERSONALI RELATIVI ALLA SALUTE PER I QUALI È RICHIESTO UN CONSENSO SPECIFICO ED ESPLICITO

ART. 7 DATI GENETICI

Il trattamento dei dati genetici da chiunque effettuato è consentito nei soli casi previsti dall'art.9, paragrafo 2 del Regolamento UE e dalle misure di garanzia approvate dal Garante per la protezione dei dati personali in attuazione dell'art. 2- septies del Codice.

I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti e accessibili ai soli soggetti autorizzati al trattamento.

Il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti. Il trasferimento dei dati in formato elettronico deve essere cifrato o, comunque, può essere effettuato nel rispetto delle disposizioni date dal Referente della UO Tecnologie Informatiche e di Comunicazione o dal Responsabile della Protezione dei dati.

ART. 8 DOSSIER SANITARIO ELETTRONICO

Il Dossier Sanitario Elettronico (DSE), attivabile a seguito di specifico ed espresso consenso, contiene i dati personali e sanitari, presenti in formato elettronico all'interno dell'archivio informatico della Azienda USL di Bologna, raccolti e prodotti da professionisti operanti presso l'Azienda USL di Bologna, volti a documentare la storia clinica del paziente interessato (cartelle cliniche dei ricoveri, verbali di Pronto Soccorso, lettere di dimissione, risultati degli esami di laboratorio e di radiologia, i referti di visite specialistiche ambulatoriali, ...). Viene alimentato nel tempo con i dati relativi ad eventi clinici dell'interessato.

Al Dossier Sanitario Elettronico può accedere, in forma protetta e riservata, solamente personale sanitario, autorizzato al trattamento, che svolga la propria attività presso le strutture sanitarie della Azienda USL di Bologna e sia, a vario titolo, direttamente coinvolto nel percorso di cura. Il DSE consente ai professionisti sanitari dell'Azienda, che prendano in cura il paziente, di disporre di un quadro di informazioni sanitarie che consenta di fornire l'assistenza più adeguata possibile.

Il Dossier può essere consultato soltanto per il tempo indispensabile ad espletare le relative operazioni di cura. I dati personali in esso contenuti non sono modificabili e sono protetti in modo da garantirne la sicurezza, la riservatezza.

Per ogni ulteriore approfondimento in materia di DSE si rinvia alla deliberazione dell'Autorità Garante per la protezione dei dati personali del 4 giugno 2015 ed alla deliberazione aziendale n.131 del 7 maggio 2018, recante "Linee di indirizzo per la gestione del Dossier Sanitario Elettronico nell'Azienda USL di Bologna" e s.m.i..

PARTE QUINTA
MISURE TECNICHE E ORGANIZZATIVE

ART. 9 MISURE ORGANIZZATIVE PER IL RISPETTO DELLA DIGNITÀ DEGLI INTERESSATI

Nel pieno rispetto dell'art.24 del Regolamento UE (Responsabilità del Titolare del trattamento) e del Provvedimento del Garante per la protezione dei dati personali del 9 novembre 2005 sul rispetto della dignità nelle Strutture sanitarie (doc. web n.1191411), nell'organizzazione delle prestazioni e dei servizi, il Titolare adotta misure di tipo organizzativo volte a garantire il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale.

Tra le principali misure di carattere organizzativo adottate, nel rinviare per ogni approfondimento alle policy di cui alle note Prot. n.141180 del 21 novembre 2018 ("Misure idonee a garantire il rispetto dei diritti dei cittadini utenti"), Prot. n.141668 del 22 novembre 2018 ("Misure e accorgimenti per la consegna di presidi sanitari al domicilio") e Prot. n. 4233 del 12 gennaio 2018 ("Modalità di consegna referti"), si richiamano:

- 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, siano erogate 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 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;
- l'adozione della procedura di gestione per l'esercizio dei diritti dell'interessato.

ART. 10 MODALITÀ DI RACCOLTA E REQUISITI DEI DATI

I Referenti Privacy, i Responsabili di trattamento ed i soggetti autorizzati al trattamento sono tenuti a trattare i dati nel rispetto delle disposizioni di cui all'articolo 5 del Regolamento UE.

ART. 11 MISURE DI SICUREZZA DI CARATTERE GENERALE

Il trattamento dei dati mediante utilizzo di strumenti tecnologici deve essere effettuato in modo da ridurre al minimo i rischi di distruzione e perdita anche accidentale dei dati stessi, di accesso non autorizzato o di

trattamento non consentito o non conforme alla qualità della raccolta, tramite l'applicazione di misure di sicurezza adottate dalla UO Tecnologie Informatiche e di Comunicazione e/o dal Responsabile della protezione dei dati - DPO, in conformità all'articolo 32 del Regolamento UE ("Sicurezza del trattamento").
Tutti i soggetti autorizzati al trattamento sono tenuti a trattare i soli dati essenziali per svolgere l'attività istituzionale, riducendo al minimo l'utilizzo di dati identificativi, in modo da escludere il trattamento quando le finalità perseguite nei singoli casi possano essere realizzate mediante l'utilizzo di dati anonimi, o mediante modalità che consentano di identificare l'interessato solo in caso di necessità.

I dati su supporto cartaceo dovranno essere conservati in luoghi e contenitori atti ad evitare perdite, sottrazioni, danneggiamenti, distruzioni e l'accesso a soggetti diversi dal personale autorizzato al relativo trattamento, nel rispetto peraltro del principio della tutela della riservatezza di terzi.
Il personale autorizzato ha accesso ai soli dati la cui conoscenza sia direttamente necessaria per adempiere ai compiti rispettivamente assegnati.

Gli atti e i documenti devono essere conservati in archivi ad accesso protetto ed i soggetti autorizzati al trattamento debbono conservarli e restituirli al termine delle operazioni effettuate.
Nel caso di trattamenti di dati particolari di cui agli articoli 9 e 10 del Regolamento UE, oltre a quanto sopra previsto, debbono essere osservate le seguenti istruzioni:

a) gli atti e documenti debbono essere conservati in locali o contenitori muniti di serratura, fino alla loro eventuale distruzione nel rispetto dei limiti temporali previsti dalle norme in materia di scarto degli atti d'archivio;
b) l'accesso agli archivi deve essere controllato e devono essere identificati e registrati i soggetti che vi accedono dopo l'orario di chiusura degli archivi stessi.

Ciascun Referente Privacy deve individuare e rappresentare all'Azienda o al Responsabile della protezione dei dati l'insieme dei beni materiali necessari per garantire la sicurezza dei dati trattati su supporto cartaceo nelle proprie articolazioni di competenza.

Per ogni singolo trattamento di dati deve essere individuata la finalità e la compatibilità con i fini istituzionali. Per le operazioni di raccolta e conservazione di dati previste da espresse disposizioni normative è richiesta l'indicazione della relativa fonte normativa.

I Referenti Privacy, anche mediante controlli periodici, sono tenuti a verificare costantemente la stretta pertinenza, non eccedenza e indispensabilità dei dati rispetto al rapporto e alla prestazione, anche con riferimento ai dati che l'interessato fornisca di propria iniziativa.

I dati che, anche a seguito delle verifiche, risultino eccedenti o non pertinenti o non indispensabili non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene.

Il trattamento dei dati, anche particolari, effettuato con strumenti elettronici è consentito solo in presenza delle seguenti misure minime garantite dalla UO Tecnologie Informatiche e di Comunicazione:

a) autenticazione informatica, con le specifiche procedure di gestione delle credenziali di autenticazione;
b) utilizzazione di un sistema di autorizzazione;
c) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito al personale autorizzato ed agli addetti alla gestione o alla manutenzione degli strumenti elettronici;
d) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
e) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
f) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale.

ART. 12 MISURE DI SICUREZZA A PROTEZIONE DEI DOCUMENTI E DEGLI ARCHIVI CARTACEI

Con riferimento al trattamento di dati personali su supporto cartaceo, tutti i soggetti autorizzati al trattamento dei dati personali devono attenersi al rispetto delle misure di sicurezza di carattere generale, indicate dal Titolare, e di carattere specifico, indicate dal Referente Privacy di riferimento.

A titolo esemplificativo, è buona norma:

- 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 soggetti 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 (ad es. sulla scrivania o su tavolini di reparto).

È compito di ciascun soggetto autorizzato al trattamento svolgere ogni operazione di trattamento dei dati personali attenendosi alle istruzioni comunicate e disponibili al link: https://www.ausl.bologna.it/privacy .

L'accesso agli archivi aziendali è controllato. 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.

ART. 13 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 con deliberazione aziendale n.146 del 19/04/2019,come aggiornata con deliberazione n. 5 dell'11/1/2023 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 nel Registro Aziendale delle Violazioni.

ART. 14 VIDEOSORVEGLIANZA

L'Azienda USL di Bologna svolge attività di videosorveglianza nel rispetto dei principi di cui agli artt. 5 e 6 del Regolamento UE 2016/679, del D.lgs. n. 196/2003 s.m.i., secondo le indicazioni fornite dal Garante per la Protezione dei dati personali con Provvedimento Generale sulla videosorveglianza dell'8.4.2010 e degli atti aziendali conseguenti.

L'istallazione presso le strutture aziendali dei sistemi di videosorveglianza è finalizzata alla tutela della sicurezza delle persone, che a vario titolo frequentano o che accedono alle stesse, e alla protezione dei dati, dei beni e del patrimonio aziendale, rispetto a possibili aggressioni, furti, rapine o atti di vandalismo e qualsiasi altro atto illecito.

I dati raccolti vengono conservati per 72 ore e sono adeguatamente protetti attraverso misure tecniche e organizzative al fine di ridurre al minimo i rischi di distruzione, di perdita anche accidentale, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità di raccolta, anche in relazione alla trasmissione delle immagini tratte o derivate da parti di videoriprese.

Tutte le aree in cui sono installati sistemi di videosorveglianza sono individuate mediante apposizione di cartelli informativi in posizione chiaramente visibile.

Le immagini sono conservate dai sistemi la cui gestione è in capo al Direttore della U.O. Tecnologie Informatiche e di Comunicazione.

L'attività di videosorveglianza è attivata ad integrazione di altre misure (es. sistemi di allarme, controlli fisici o logistici, misure di protezione agli ingressi).

PARTE SESTA
TUTELA DELL'INTERESSATO

ART. 15 DIRITTI DELL'INTERESSATO

L'Azienda USL di Bologna, in qualità di Titolare del trattamento dei dati personali, ha l'obbligo di rendere note le modalità per l'esercizio dei diritti da parte degli interessati in forma concisa, trasparente, intelligibile e facilmente accessibile, ricorrendo ad un linguaggio semplice e chiaro, così come previsto dall'art.12 del Regolamento UE.

Con la deliberazione aziendale n.7 dell'11/1/2023 ("Procedura per la Gestione dell'esercizio dei diritti dell'interessato") sono state aggiornate le modalità operative adottate dall'Azienda USL di Bologna, al fine di agevolare e garantire la gestione delle richieste di esercizio dei diritti dell'interessato, relativamente al trattamento dei dati personali, in maniera standardizzata e nel rispetto di quanto previsto dalla normativa.

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.12-21 del Regolamento UE, esercitando i diritti:

- di informazione, comunicazione e trasparenza (artt.12, 13 e 14);
- 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).

L'Azienda USL di Bologna fornisce all'interessato le informazioni relative alle richieste ai sensi degli artt. da 15 a 22 del Regolamento (UE) 2016/679 senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa.

Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste.

In questo caso, il DPO, entro un mese dal ricevimento della richiesta, informa l'interessato della necessità di prorogare l'inoltro della risposta dando conto dei motivi del ritardo e della possibilità di proporre reclamo all'Autorità di controllo e di proporre ricorso giurisdizionale.

La procedura per la gestione di violazioni nel trattamento dei dati personali è stata ampiamente diffusa a tutto il personale e pubblicata sul sito web aziendale all'interno della sezione *privacy policy* https://www.ausl.bologna.it/privacy/i-diritti-degli-interessati .

ART. 16 COMUNICAZIONE DI DATI PERSONALI

Fermo restando quanto previsto dalle norme di cui al Regolamento UE e al Codice, non configura *comunicazione dei dati* il trasferimento degli stessi alle diverse strutture dell'Azienda USL di Bologna.

ART. 17 MODALITÀ SEMPLIFICATE PER L'INFORMAZIONE AL PAZIENTE

Con riferimento al trattamento dei dati per finalità di diagnosi, assistenza, terapia sanitaria o sociale, l'Azienda USL di Bologna è tenuta a rendere le informazioni previste dagli articoli 13 e 14 del Regolamento UE secondo le modalità concordate con il Responsabile della Protezione dei Dati.

In ogni caso, tali informazioni dovranno essere fornite al momento dell'accesso alla prestazione sanitaria, anche sinteticamente, ma con rinvio alla apposita sezione del sito internet aziendale ed alle informazioni affisse nelle zone di accesso e transito dei pazienti.

ART. 18 ULTERIORI MODALITÀ DI TRATTAMENTO DEI DATI PARTICOLARI

Al fine di garantire il rispetto dei diritti, delle libertà fondamentali, della dignità, della riservatezza e della protezione dei dati degli interessati, nonché del segreto professionale, all'interno di ogni struttura erogatrice di prestazioni sanitarie dell'Azienda USL di Bologna sono adottate ulteriori misure tecniche e organizzative, oltre a quelle richiamate nella parte prima delle presenti Linee Guida, atte a garantire la protezione dei dati trattati.

Per l'utilizzo a fini amministrativi, dovrà essere rilasciata copia del referto di esami specialistici non contenente alcun riferimento diagnostico.

Fermo restando quanto sopra previsto, i dati idonei a rivelare lo stato di salute possono essere resi noti agli interessati solo per il tramite di un medico.

La copia della cartella clinica e di altra documentazione sanitaria deve essere consegnata all'interessato (o a persona munita di apposita delega sottoscritta dall'interessato) in busta chiusa nel rispetto delle misure adottate dal Titolare, contenute nella nota già richiamata e pubblicata all'interno della sezione *privacy policy* (nota Prot. n.4233 del 12 gennaio 2018).

Eventuali richieste di presa visione o di rilascio di copia della cartella clinica o dell'acclusa scheda di dimissione ospedaliera 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 far valere o difendere un diritto in sede giudiziaria di rango almeno pari a quello dell'interessato e, quindi, consistente in un diritto della personalità o in un altro diritto o libertà fondamentale ed inviolabile;
- di tutelare, in conformità alla disciplina sull'accesso ai documenti amministrativi, una situazione giuridicamente rilevante di rango almeno pari a quella dell'interessato o consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile.

ART. 19 ALTRE MISURE OPERATIVE IN MATERIA DI DATI PERSONALI

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

Il Referente Privacy cura che:

- le fotocopiatrici ed i fax siano collocati in un'area protetta e presidiata 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 vigenti linee guida aziendali 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.

PARTE SETTIMA
DISPOSIZIONI FINALI

ART. 20 FORMAZIONE

L'Azienda USL di Bologna individua nella formazione del personale un elemento strategico della propria politica in materia di protezione dei dati personali.

La formazione, individuata quale formazione obbligatoria, può essere erogata sia ricorrendo a risorse interne sia avvalendosi di risorse esterne e può avvenire attraverso modalità di e-learning.

Nell'ambito della programmazione degli interventi di formazione del personale, sono garantiti a tutto il personale, in relazione ai distinti ruoli, interventi di formazione, in materia di protezione dei dati personali e corretto trattamento e tutela della riservatezza, finalizzati alla conoscenza della normativa, all'adozione di idonei modelli di comportamento e procedure di trattamento, alla conoscenza dei rischi e delle misure di sicurezza per prevenirli.

ART. 21 ATTIVITÀ DI AUDIT

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.

ART. 22 DISPOSIZIONI FINALI

Ogni qualvolta sussistano 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 il normale espletamento delle attività. In ogni caso, il personale autorizzato è tenuto a rivolgersi al Referente Privacy di afferenza, il quale può avvalersi del supporto del Responsabile della Protezione dei dati - DPO.

Per tutto quanto non espressamente previsto dalle presenti Linee Guida si rinvia alle disposizioni europee, nazionali, regionali ed aziendali in materia.