1182

REGOLAMENTO AZIENDALE SUL TRATTAMENTO DEI DATI PERSONALI

Regolamento UE 2016/679 (Regolamento generale sulla protezione dei dati)

Delibera n. del

Oggetto:

Il presente Regolamento sulla privacy è uno strumento di applicazione della vigente normativa in materia di tutela dei dati personali e sensibili nell'ambito dell'organizzazione aziendale e contiene, pertanto, le disposizioni in materia di riservatezza dei dati personali adottate da questa Azienda Socio Sanitaria Territoriale (d'ora innanzi ASST) al fine di adeguare l'organizzazione interna a quanto stabilito dal legislatore nazionale e europeo.

Attraverso la diffusione capillare del presente documento si intende perseguire la finalità di supportare i Responsabili e gli Incaricati del trattamento nel corretto svolgimento delle attività di trattamento dati, affinché le stesse si svolgano nel pieno rispetto sia della normativa privacy vigente sia dei criteri di funzionalità ed efficienza a cui deve essere improntata l'attività lavorativa.

Destinatari:

I destinatari del documento sono i Responsabili e gli Incaricati, designati e autorizzati dall'ASST a svolgere operazioni di trattamento in ambito sanitario e/o amministrativo.

Riferimenti normativi

La redazione del presente documento è stata effettuata sulla base delle seguenti fonti normative:

- Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (d'ora innanzi GDPR), 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);

- D.Lgs. 30 giugno 2003, n. 196, così come modificato dal D.Lgs. 101/2018: "Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 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 dei dati e che abroga la direttiva 95/46/CE";
- Regolamento Regionale 24 dicembre 2012, n. 3: "Regolamento per il trattamento dei dati sensibili e giudiziari di competenza della Giunta regionale, delle aziende sanitarie, degli enti e agenzie regionali, degli enti vigilati dalla Regione Lombardia" (pubblicato sul BURL n. 52, suppl. ord. del 27 dicembre 2012);
- provvedimenti, relazioni e comunicati stampa del Garante Privacy: si citano, in via esemplificativa e non esaustiva:
  - Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati" (pubblicato sulla Gazzetta Ufficiale n. 134 del 12 giugno 2014);
  - Linee guida in materia di Dossier sanitario - 4 giugno 2015 (pubblicato sulla Gazzetta Ufficiale n. 164 del 17 luglio 2015);
- codici di deontologia professionale;
- atti, procedure e modelli aziendali;
- norme comportamentali desunte dalla miglior prassi.

Al fine di garantirne l'efficace e corretta applicazione, l'Azienda Socio Sanitaria Territoriale Fatebenefratelli Sacco procederà al periodico aggiornamento e monitoraggio del presente documento.

6

INDICE

Oggetto, destinatari e rifermenti normativi

Sezione 1 Definizioni

Sezione 2 Le figure aziendali di riferimento per la tutela dei dati personali

Il titolare del trattamento

Il responsabile del trattamento

Gli incaricati del trattamento

Ambito di trattamento

Le figure aziendali di riferimento

Sezione 3 Informativa – Consenso – Diritti dell'Interessato

Informativa

Consenso

I diritti dell'interessato

Sezione 4 Trattamento dei dati personali in ambito sanitario. Altre misure per il rispetto dei diritti dell'interessato

Sezione 5 Altre disposizioni

Sezione 6 Valutazioni di impatto, Responsabile della protezione dei dati, Registro delle attività di trattamento, Sanzioni

Sezione 1 - DEFINIZIONI

Per **Regolamento** si intende il Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (d'ora innanzi anche GDPR), 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). Con riferimento al Regolamento si specifica che la sua pubblicazione è avvenuta in data 4 maggio 2016 e che, a partire dal giorno della pubblicazione, gli Stati membri hanno avuto due anni di tempo per allineare la normativa nazionale alle nuove prescrizioni introdotte dal Regolamento, che è divenuto definitivamente applicabile in tutto il territorio UE a partire dal 25 maggio 2018.

Per **Trattamento** dei dati si intende qualunque 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 (articolo 4, comma 2, GDPR).

Esempi di trattamento svolti durante le attività Aziendali sono:

- l'introduzione dei dati anagrafici del paziente durante l'applicazione della procedure di prenotazione/accettazione nel sistema informativo dell'Azienda;
- l'introduzione dei dati anagrafici dei fornitori nel sistema informativo dell'Azienda,
- l'introduzione di dati anagrafici dei dipendenti nel sistema informativo dell'Azienda;
- la visualizzazione su video di dati di utenti, dipendenti e fornitori (es. gestione appuntamenti, cedolino stipendiale, controlli contabili ecc.);
- la stampa di documenti contenenti dati personali, la loro consegna all'utente/destinatario, la loro eliminazione in caso di errata emissione;
- il trasporto di documenti cartacei quali cartelle cliniche, referti, certificati, fatture, ecc.;
- la consultazione, la riorganizzazione, l'archiviazione dei documenti e la loro gestione negli archivi;
- la registrazione di informazioni nella cartella clinica e/o nei registri di attività sanitaria.

Pertanto, anche l'attività di semplice custodia o conservazione dei dati personali rientra nel concetto di trattamento ed è soggetta alle disposizioni previste dalla normativa.

Il trattamento è dunque qualunque tipo di gestione dei dati, dalla loro **nascita** (data

input, scrittura su carta), all'**utilizzo** (visualizzazione, comunicazione, emissione, modifica, archiviazione) sino alla **fine** (cancellazione, distruzione).

Per **Dato personale** si intende qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (articolo 4, comma 1, GDPR).

Per **Dati relativi alla salute** si intendono i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute (articolo 4, comma 15 GDPR).

Per **Dati genetici** si intendono i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione (articolo 4, comma 13 GDPR).

Per **Dati biometrici** si intendono i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici (articolo 4, comma 14 GDPR).

Per **Violazione** dei dati personali si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati (articolo 4, comma 12 GDPR).

Per **Titolare** del trattamento si intende 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 (articolo 4, comma 7 GDPR).

Per **Responsabile del trattamento** si intende la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare

del trattamento (articolo 4, comma 8 GDPR).

Per **Incaricati** si intendono le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.

Per **Interessato** s'intende la persona fisica, cui si riferiscono i dati personali.

Per **Dato anonimo** si intende il dato che in origine, o a seguito del trattamento, non può essere associato ad un interessato identificato o identificabile.

Per **Profilazione** si intende qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti 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 (articolo 4, comma 4 GDPR).

Per **Pseudonimizzazione** si intende il trattamento dei dati personali in modo tale che i dati personali non possano essere più 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 un persona fisica identificata o identificabile (articolo 4, comma 4 GDPR).

Per **Garante** s'intende l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675

.

10

Sezione 2 - LE FIGURE AZIENDALI DI RIFERIMENTO PER LA TUTELA DEI DATI PERSONAL

Il TITOLARE DEL TRATTAMENTO (art. 4, comma 7 GDPR)

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, ivi compreso il profilo della sicurezza; n**el caso specifico è l'Azienda Socio Sanitaria Territoriale Fatebenefratelli Sacco** ad essere titolare del trattamento nella sua persona giuridica, ma ne risponde il Direttore Generale in quanto legale rappresentante.
Il titolare del trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento UE e al D.lgs 196/2003 e ss.mm.ii.
Si indicano di seguito i **compiti del Titolare:**

1) attuare gli obblighi in materia di protezione del trattamento dei dati;
2) designare, se lo ritiene, uno o più responsabili del trattamento;
3) vigilare sulla puntuale osservanza delle istruzioni loro impartite;
4) formare il personale.

L'Azienda, nella sua qualità di Titolare del trattamento, nomina i **Responsabili del Trattamento**:

- il Direttore Amministrativo, il Direttore Sanitario, il Direttore Socio Sanitario e il Direttore Medico di Presidio, ciascuno per le banche date e gli archivi gestiti negli ambiti di rispettiva competenza;
- per l'area sanitaria: i direttori di Struttura Complessa e i responsabili di Struttura Semplice Dipartimentale e di staff, ciascuno per le banche dati e gli archivi gestiti negli ambiti di rispettiva competenza;
- per l'area amministrativa: i direttori di Struttura Complessa e i responsabili di Struttura Semplice dipartimentale e di staff, ciascuno per le banche dati e gli archivi gestiti negli ambiti di rispettiva competenza;
- per la gestione del sistema di videosorveglianza preposti a tutela del patrimonio e della sicurezza: il Direttore della UOC Sistema Informativo Ospedaliero e Organizzazione (SIOO);
- per la gestione degli impianti di videosorveglianza predisposti al controllo di ambienti sanitari e monitoraggio clinico di pazienti: Direttore di Struttura Complessa/Responsabile di Struttura Semplice nel cui ambito è installato l'impianto medesimo, in virtù della nomina effettuata dall'ASST.

- i soggetti esterni all'Azienda, per qualsivoglia forma di "outsourcing" che comporti un trattamento di dati personali/sensibili.

Le nomine dei Responsabili interni dell'Azienda, a firma del Direttore Generale, vengono predisposte dalla UOC Organizzazione e Risorse Umane all'atto dell'assunzione, la quale provvederà ad archiviare le stesse nel fascicolo personale. Una copia della nomina sarà trattenuta dal Responsabile interno nominato ed un'altra inviata alla UOC Affari Generali e Legali.

Le nomine dei Responsabili esterni dell'Azienda, a firma del Direttore Generale, vengono predisposte, secondo l'apposito modello, dai **Responsabili del procedimento** all'atto della stipula del contratto/ordine.
Il modulo di designazione della nomina, sottoscritto dal Responsabile del trattamento dei dati della società o persona fisica fornitrice, sarà conservato con il contratto/ordine. Una copia sarà trattenuta dal soggetto esterno nominato ed un'altra inviata all'UOC Affari Generali e Legali.

IL RESPONSABILE DEL TRATTAMENTO:
è la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che tratta dati personali per conto del titolare del trattamento.
Il Responsabile deve essere designato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.
I compiti affidati al Responsabile sono analiticamente specificati per iscritto dal Titolare.

Responsabile interno: compiti
Quali responsabili interni del trattamento sono individuati i Direttori delle strutture complesse/i Responsabili delle Strutture Semplici Dipartimentali e delle Strutture Semplici di staff, secondo l'area (sanitaria o amministrativa) di competenza come sopra precisato.
Ai citati Responsabili vengono affidati i seguenti compiti:

- **procedere** al trattamento dei dati personali, sensibili e giudiziari, secondo le istruzioni impartite dal Titolare del trattamento (nella figura del Legale Rappresentante dell'ASST), nel pieno rispetto delle vigenti disposizioni in materia;
- **nominare** per iscritto i propri collaboratori "Incaricati del trattamento" **archiviare** le avvenute nomine dei propri collaboratori e **provvedere** al costante aggiornamento delle stesse sulla base della dotazione organica;
- **individuare** e **aggiornare** gli ambiti di trattamento consentiti e **comunicarli** agli incaricati;

12

- **vigilare** affinché il personale incaricato del trattamento operi in conformità alle disposizioni di legge e ai regolamenti loro impartiti;
- **vigilare** affinché ogni dato, elenco o banca dati cartacea, informatica e telematica venga trattato per i soli fini per i quali è stato raccolto;
- **vigilare** affinché i documenti contenenti dati personali e sensibili vengano custoditi in modo da non essere accessibili a persone non incaricate del trattamento;
- **controllare** che i dati personali, sensibili e giudiziari, vengano comunicati nel rispetto delle prescrizioni impartite; i documenti contenenti dati personali e sensibili non devono essere condivisi, comunicati o inviati a persone non autorizzate;
- **verificare** che l' informativa di cui agli articoli 13 e 14 del Regolamento UE venga effettivamente resa;
- **controllare** che gli incaricati raccolgano il consenso dell'interessato (nei casi previsti dalla legge) per il trattamento dei dati personali e sensibili;
- **vigilare** affinché i dati personali, sensibili e giudiziari, raccolti su supporti cartacei ed informatici vengano trattati nel rispetto delle misure minime di sicurezza di cui all'art. 32 del Regolamento UE.

In particolare si rammenta che la nomina dell'incaricato deve essere posta in essere al momento della presa in carico del personale all'interno delle proprie strutture e che le nomine devono essere aggiornate in base alla dotazione organica.
Le lettere di nomina firmate, con le relative **istruzioni operative** e **l'ambito di trattamento**, devono essere archiviate all'interno della Struttura aziendale di appartenenza.

Responsabile esterno: compiti

I Responsabili esterni del trattamento sono individuati nelle persone fisiche e giuridiche che, nell'esercizio delle proprie funzioni, trattano dati personali/sensibili per conto dell'ASST (es. società di software, consulenti ect...)

Ai Responsabili esterni vengono affidati i seguenti compiti:

- **procedere** al trattamento dei dati personali, sensibili e giudiziari, secondo le istruzioni impartite dal Titolare del trattamento (nella figura del Legale Rappresentante dell'ASST), nel pieno rispetto delle vigenti disposizioni in materia;
- **nominare** per iscritto i propri collaboratori "Incaricati del trattamento", **provvedere** al costante aggiornamento delle nomine stesse sulla base della dotazione organica e farne pervenire copia al Titolare del trattamento;
- **individuare** e **aggiornare** gli ambiti di trattamento consentiti e **comunicarli** agli incaricati;

- **vigilare** affinché il personale incaricato del trattamento operi in conformità alle disposizioni di legge e ai regolamenti loro impartiti;
- **vigilare** affinché ogni dato, elenco o banca dati cartacea, informatica e telematica venga trattato per i soli fini per i quali è stato raccolto;
- **vigilare** affinché i documenti contenenti dati personali vengano custoditi in modo da non essere accessibili a persone non incaricate del trattamento;
- **controllare** che i dati personali, sensibili e giudiziari, vengano comunicati nel rispetto delle prescrizioni impartite; i documenti contenenti dati personali e sensibili non devono essere condivisi, comunicati o inviati a persone non autorizzate;
- **vigilare** affinché i dati personali, sensibili e giudiziari, raccolti su supporti cartacei ed informatici vengano trattati nel rispetto delle misure minime di sicurezza di cui all'articolo 32 del Regolamento UE.

Si ricorda inoltre che gli obblighi relativi alla riservatezza dovranno essere osservati anche in seguito a modifica dell'incarico e/o cessazione del rapporto di lavoro e che la nomina a Responsabile cesserà automaticamente con il venir meno del rapporto intercorrente tra il Titolare (ASST Fatebenefratelli Sacco) ed il Responsabile.

GLI INCARICATI AL TRATTAMENTO:
Gli "incaricati del trattamento" sono le **persone fisiche** che effettuano materialmente le operazioni di trattamento dei dati personali e sensibili ed operano sotto la diretta autorità del Responsabile.

Compiti:
Gli Incaricati del trattamento devono, in ogni operazione del trattamento, garantire la massima riservatezza ed osservare le seguenti istruzioni a seconda della pertinenza e del ruolo assegnato (sanitari o amministrativi):

in particolare per la protezione dei documenti cartacei:

1) i documenti oggetto di trattamento possono essere affidati soltanto a **soggetti appositamente autorizzati** e nel rispetto del proprio ambito di trattamento;
2) durante il trattamento i documenti devono essere **custoditi e controllati** in modo che ad essi non accedano persone prive di autorizzazione, in particolare non devono rimanere incustoditi su scrivanie o tavoli di lavoro;
3) concluso il trattamento, i documenti devono essere collocati in una **stanza presidiata dal personale autorizzato** o - se la stanza non è presidiata, i documenti devono essere collocati in un armadio chiudibile o nella stessa stanza chiudibile;

4) in caso di interruzione, anche temporanea, del lavoro, verificare che i dati trattati non siano accessibili a terzi non autorizzati;
5) in occasione della **trasmissione dei documenti che avviene all'esterno dell'Azienda** devono essere adottati tutti gli accorgimenti necessari e idonei onde evitare che le informazioni riservate possano essere lette, sia pure accidentalmente, da chi non è autorizzato (ad esempio trasporto mediante cartelle chiuse);
6) in occasione della trasmissione dei documenti agli interessati, gli stessi devono essere risposti **in busta chiusa,** priva all'esterno di informazioni sensibili, da consegnarsi direttamente all'Interessato o al terzo delegato per iscritto;
7) i documenti recanti dati genetici possono essere trattati **esclusivamente all'interno di locali protetti** accessibili ai soli incaricati ed ai soggetti specificatamente autorizzati ad accedervi;
8) i documenti recanti dati genetici possono essere trasportati all'esterno dai locali riservati al loro trattamento soltanto mediante **contenitori muniti di serratura** o altri dispositivi equipollenti;
9) i documenti **non devono essere riciclati** (ad esempio per carta da minuta o per le fotocopie) onde evitare il rischio che gli stessi possano essere letti da chi non è autorizzato;
10) i documenti contenenti dati personali e sensibili **devono essere eliminati** utilizzando gli appositi apparecchi "distruggi documenti" o, in assenza, sminuzzati in modo da non essere più ricomponibili;
11) i documenti possono essere affissi in stanze ad accesso selezionato a condizione che siano posizionati in modo tale da **evitare che le informazioni possano essere lette sia pure accidentalmente da chi non è autorizzato** (ad esempio, sulla parte interna dell'anta di una armadio, in un cassetto, eccetera).
12) raccogliere, registrare e conservare i dati presenti nella documentazione (sanitaria/amministrativa) della UOC/UOS di appartenenza e nei supporti informatici avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;
13) è vietata la diffusione dei dati;
14) è vietata la comunicazione dei dati senza la preventiva autorizzazione del Responsabile;
15) l'accesso ai dati dovrà essere limitato all'espletamento delle proprie mansioni ed esclusivamente negli orari di lavoro;

in particolare per la protezione della persona:

1) in sala d'attesa devono essere adottate modalità di **chiamata del paziente** che prescindano dalla sua individuazione nominativa (contatto diretto, numero, tabellone elettronico);

45

2) in sala d'attesa deve essere istituita la **distanza di cortesia** tra utente allo sportello e utente in fila e, se ciò non è realizzabile per le dimensioni della stanza, deve essere adottato un comportamento improntato alla massima prudenza onde evitare l'indebita conoscenza da parte di terzi di informazioni idonee a rivelare lo stato di salute del paziente;
3) i **colloqui sanitari** devono svolgersi in locali protetti e, qualora ciò non sia possibile, deve essere adottato un comportamento improntato alla massima prudenza onde evitare l'indebita conoscenza da parte di terzi di informazioni idonee a rivelare lo stato di salute del paziente;
4) la prestazione sanitaria, compresa l'eventuale documentazione di anamnesi, deve avvenire in **assenza di situazioni di promiscuità** derivanti dalle modalità o dai locali prescelti;
5) la prestazione deve essere erogata nel rispetto della **dignità del paziente**, soprattutto in riferimento a fasce deboli (minori, disabili, anziani) o situazioni particolari (interruzione della gravidanza, patologie quali hiv/aids) che richiedono particolare sensibilità;
6) gli operatori sanitari che, nell'esercizio della loro professione, vengono a conoscenza di un caso di AIDS, ovvero di un caso di HIV, anche non accompagnato da stato morboso, devono adottare tutte le misure occorrenti per la tutela della riservatezza, e comunicare i risultati degli accertamenti diagnostici, diretti o indiretti, esclusivamente, alla persona cui tali esami sono riferiti (art. 5, commi 1 e 4, Legge 135/1990);
7) **il paziente deve essere debitamente** informato **prima dell'acquisizione del consenso al trattamento dei dati personali e sensibili;**
8) devono essere rispettate le **indicazioni formulate dal paziente** nei modelli aziendali circa i **soggetti autorizzati a ricevere comunicazioni sullo stato di salute;**
9) deve essere prevenuto il rischio che gli estranei possano collegare il paziente al suo stato di salute: ad esempio **non contrassegnare** la carrozzella o la barella che trasporta il paziente con l'indicazione del reparto di provenienza, così come nella spedizione di prodotti o documenti non indicare, sulla parte esterna del plico postale, informazioni idonee a rivelare l'esistenza di uno stato di salute dell'interessato (ad es., indicazione della tipologia del contenuto del plico o del reparto dell'organismo sanitario mittente);
   Tali cautele devono essere orientate anche alle eventuali certificazioni richieste per fini amministrativi non correlati a quelli di cura (ad es., per giustificare un'assenza dal lavoro o l'impossibilità di presentarsi ad una procedura concorsuale);

<u>in particolare per la protezione dei documenti informatici:</u>

1) utilizzare password riservate e personalizzate per l'accesso ai sistemi informatizzati;

16

2) la password deve essere composta da almeno **otto caratteri** o, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito;
3) nella password **non devono essere immessi riferimenti agevolmente riconducibili alla propria persona** (ad esempio nome, cognome, data di nascita);
4) la password deve essere **modificata al primo utilizzo** e, successivamente, almeno ogni sei mesi; in caso di trattamento di dati sensibili e di dati giudiziari modificare la password almeno ogni tre mesi;
5) la password **non deve essere trascritta su promemoria** in vista (ad esempio biglietti dinanzi al pc o affissi in bacheca) o comunicata a terzi;
6) non installare e non scaricare da Internet programmi non pertinenti l'attività lavorativa né qualsiasi altro programma, senza la preventiva autorizzazione da parte della UOC Sistema Informativo Ospedaliero ed Organizzazione (SIOO) Sistemi Informativi e Supporto Organizzativo ;
7) comunicare tempestivamente alla UOC l'eventuale rilevazione di anomalie nell'utilizzo del sistema informatico che possono compromettere la sicurezza dei dati;
8) verificare la provenienza dei messaggi di posta elettronica contenenti allegati e cancellare direttamente quelli di dubbia provenienza;
9) utilizzare la posta elettronica e la connessione ad Internet esclusivamente per lo svolgimento dei propri compiti istituzionali;
10) non diffondere messaggi di posta elettronica (es: catena di S. Antonio).

AMBITO DI TRATTAMENTO

E' definito, per tutto il **personale sanitario e non sanitario** operante presso i reparti di degenza - ambulatori - servizi sanitari, l'ambito di trattamento consentito ai Responsabili e Incaricati su tutta la **documentazione sanitaria**. Nella tabella sono riportate le figure che possono/non possono trattare i documenti sanitari e sono stati definiti i trattamenti possibili. La tabella deve essere portata a conoscenza, da parte del Responsabile del trattamento, di tutti gli operatori dei reparti di degenza - ambulatori - servizi sanitari.
Analogamente, **il Responsabile di ciascuna struttura amministrativa** definisce l'ambito di trattamento, consentito agli Incaricati, dei dati che possono essere trattati presso la UO di pertinenza, dandone conoscenza a tutto il Personale.

Di seguito riportiamo lo schema organizzativo posto in essere dalla ASST Fatebenefratelli Sacco.
L'Azienda ha mantenuto una verticalizzazione delle responsabilità all'interno dell'attività di gestione

TITOLARE DEL TRATTAMENTO

Azienda Socio Sanitaria Fatebenefratelli Sacco

↓

Nomina

RESPONSABILE DEL TRATTAMENTO

Direttore Sanitario per tutti i Servizi/Uffici in staff alla Direzione Sanitaria in cui non sia stato nominato un Responsabile. **Direttore Socio Sanitario** per tutti i Servizi/Uffici in staff alla Direzione Socio Sanitaria in cui non sia stato nominato un Responsabile. **Direttore Amministrativo** per tutti i Servizi/Uffici in staff alla Direzione Amministrativa in cui non sia stato nominato un Responsabile. **Direttore Medico di Presidio** per tutte le banche dati, gli archivi e le attività che rientrano nella propria competenza. **Direttori/Responsabili delle Unità Operative Ospedaliere,** per quanto riguarda le Unità Operative/Servizi Sanitari (Strutture complesse e semplici). Laddove siano installati sistemi di videosorveglianza per il controllo di ambienti sanitari e il monitoraggio clinico dei pazienti **i Direttori/Responsabili delle Unità Operative Sanitarie** sono anche responsabili del trattamento in relazione al funzionamento dei predetti sistemi.	**Responsabili esterni** (i soggetti esterni all'Azienda, per svariate forme di "outsourcing" che comportano un trattamento di dati personali/sensibili).

Direttori/Responsabili delle Unità Operative territoriali, per quanto riguarda le Unità Operative/Servizi Sanitari afferiti dal territorio in attuazione del "Progetto Milano"(Strutture complesse e semplici). **Direttori/Responsabili Amministrativi** per quanto riguarda le Unità Operative/Uffici amministrativi (Strutture complesse e semplici). **Direttore UOC SIOO** deputato "alla gestione e alla manutenzione degli strumenti elettronici" all'adozione delle "misure minime" di sicurezza ovvero del "complesso delle misure tecniche, informative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto dall'articolo 32 del GDPR. Responsabile altresì del sistema di videosorveglianza preposto a tutela del patrimonio e della sicurezza.	

Nomina

INCARICATO DEL TRATTAMENTO

Tutto il **Personale dipendente e non** che quotidianamente tratta i dati su supporto cartaceo e/o informatico.	Tutti i collaboratori che quotidianamente trattano i dati dell'ASST su supporto cartaceo e/o informatico nell'ambito delle funzioni di cui al contratto/ordine/convenzione

Sezione 3 - INFORMATIVA - CONSENSO - DIRITTI DELL'INTERESSATO

INFORMATIVA DA RENDERE QUANDO I DATI PERSONALI SONO RACCOLTI PRESSO L'INTERESSATO (artt. 13 del GDPR)

L'**informativa** è quello strumento che rende esplicita e trasparente la gestione delle informazioni di carattere personale e sensibile degli interessati ed in tal modo consente agli stessi soggetti di prendere parte attiva alla difesa dei propri diritti nell'ambito della protezione dei dati personali.

Per questo motivo l'ASST informa preventivamente l'interessato per iscritto tramite un'idonea informativa, che contiene:

- l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
- i dati di contatto del responsabile della protezione dei dati;
- le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
- qualora il trattamento sia necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, i legittimi interessi perseguiti dal titolare o da terzi;
- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
- ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali ad un paese terzo o a una organizzazione internazionale, con le garanzie indicate nel GDPR;

Nel momento in cui i dati personali sono ottenuti, sono fornite all'interessato le seguenti ulteriori informazioni:

- il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- l'esistenza del diritto dell'interessato di chiedere l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
- l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
- il diritto di proporre reclamo al Garante;
- se la comunicazione dei dati personali è un obbligo legale o contrattuale oppure se è un requisito necessario per la conclusione del contratto, e se l'interessato ha l'obbligo di fornire i dati personali, nonché le possibili conseguenze previste di tale trattamento per l'interessato;
- l'esistenza (eventuale) di un processo decisionale automatizzato, compresa la profilazione di cui all'art. 22, paragrafi 1 e 4 del GDPR e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

INFORMATIVA DA RENDERE QUANDO I DATI PERSONALI NON SONO RACCOLTI PRESSO L'INTERESSATO (artt. 14 del GDPR)

L'ASST informa preventivamente l'interessato per iscritto tramite un'idonea informativa, che contiene:

- l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
- i dati di contatto del responsabile della protezione dei dati;
- le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
- le categorie di dati personali in questione;
- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
- ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali ad un paese terzo o a una organizzazione internazionale, con le garanzie indicate nel GDPR;

Oltre a quelle sopra indicate, vengono fornite all'interessato anche le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente nei confronti dell'interessato:

- il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- qualora il trattamento sia necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, i legittimi interessi perseguiti dal titolare o da terzi;
- l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano e di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
- l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
- il diritto di proporre reclamo al Garante;
- la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico;
- l'esistenza (eventuale) di un processo decisionale automatizzato, compresa la

profilazione di cui all'art. 22, paragrafi 1 e 4 del GDPR e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

L'ASST adempie all'obbligo di informativa sia mediante la predisposizione di un modello cartaceo contenente le sopra indicate informazioni sia mediante l'affissione dello stesso in punti della struttura accessibili e ben visibili dall'utenza: ufficio accettazione e ricoveri, CUP, bacheche informative, l'ingresso ai reparti, sale d'attesa per il pubblico.
L'informativa è data per l'insieme dei trattamenti che possono essere effettuati sui dati dall'ASST.
Ciò comporta che l'informativa data all'inizio del trattamento (ad esempio all'atto del ricovero o della prenotazione della visita ambulatoriale), legittima l'insieme delle prestazioni e dei trattamenti correlati.
Il modello di informativa sopra citato è stato elaborato nel modo più esaustivo possibile, salvo il dovere del medico di integrare - con delucidazioni orali - eventuali richieste di chiarimento da parte dell'Interessato (ad esempio in caso di trattamenti particolari come la registrazione).
Peraltro si evidenzia che, a fronte di situazioni particolarmente gravi, l'obbligo di informativa può essere rimandato ad un momento successivo all'erogazione dell'urgente prestazione. Trattasi delle situazioni di:

- emergenza sanitaria;
- igiene pubblica;
- impossibilità fisica, incapacità di agire o di intendere o di volere dell'Interessato[1];
- rischio grave, imminente ed irreparabile per la salute o l'incolumità fisica dell'Interessato;
- prestazione medica che può essere pregiudicata se non è eseguita subito;
- trattamento sanitario obbligatorio.

L'ASST predispone le adeguate informative. Si citano le seguenti a titolo esemplificativo:
a. Informativa per il trattamento dei dati personali e sensibili (paziente) -: tale informativa è esposta in maniera visibile nei diversi punti di accesso alla struttura (punti accettazione ambulatoriale, PS, sale d'aspetto, CUP etc.) e pubblicata sul sito internet, nonché sulla intranet dell'Azienda.
b. Informativa per il trattamento dei dati genetici: tale informativa è consegnata al paziente nel caso vengano trattati dati genetici.

[1] Quando non è possibile acquisire il consenso da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'Interessato.

c. Informativa per il trattamento dei dati personali (personale dipendente) -: la modulistica è consegnata a tutti i dipendenti all'atto dell'assunzione.
d. Informativa per il trattamento dei dati personali (fornitore) - tale informativa è inserita nel contratto/convenzione/ordine sottoscritto, è pertanto consegnata a tutti i fornitori dell'ASST dalla UO che attiva il contratto; inoltre la stessa è disponibile anche sul sito internet dell'ASST.
e. Informativa al trattamento di fotografie/immagini (paziente) -: poiché l'utilizzo delle fotografie/immagini (che permettono l'identificazione della persona) costituisce "trattamento" di dati personali, è assolutamente vietato per chiunque effettuare riprese video e/o fotografiche all'interno dell'ASST senza la preventiva autorizzazione in forma scritta da parte dell'interessato. Le fotografie/immagini associate al cognome e nome dell'interessato, ad una sua caratteristica biometrica, sono considerate dati personali sensibili a cui vanno applicate le disposizioni di sicurezza previste in merito dalla vigente normativa.
A titolo esemplificativo, rientrano in questa fattispecie i seguenti tipi di immagine:

- le registrazioni video eventualmente effettuate durante gli interventi chirurgici (nel caso in cui sia inquadrato il volto dell'interessato);
- le immagini acquisite tramite macchina fotografica.

Qualora fosse necessario acquisire una immagine che riprenda tutto il corpo del paziente, compreso il volto, il personale medico di reparto consegna all'interessato (paziente) il modulo contenente l'informativa e la raccolta del consenso al trattamento delle fotografie/immagini.
Il modulo diventa parte integrante di tutta la documentazione che costituisce la cartella clinica. Non è necessario raccogliere il consenso, se le fotografie/immagini (per esempio le immagini radiodiagnostiche) costituiscono parte integrante dei trattamenti clinici e strumentali, a valenza sia diagnostica che terapeutica, che si rendano necessari per la cura del paziente. In questo caso il consenso è stato già ottenuto al momento dell'accettazione amministrativa per le prestazioni sanitarie.
f. Informativa Area Videosorvegliata: per ragioni di sicurezza, l'ASST ha installato telecamere, nel rispetto delle norme previste dalla normativa applicabile in materia.
I cittadini che transitano nelle aree video sorvegliate sono informati per mezzo di cartellonistica dal titolo **Area Videosorvegliata**.
g. policy privacy: è l'informativa che viene resa agli utenti che hanno accesso e navigano sul sito web dell'ASST.

<u>CONSENSO</u> (art. 7 GDPR)
Gli esercenti le professioni sanitarie e gli organismi sanitari pubblici, anche nell'ambito di un'attività di rilevante interesse pubblico trattano i dati personali idonei a rilevare lo stato di salute:

a) con il consenso dell'interessato e anche senza l'autorizzazione del Garante, se il trattamento riguarda dati e operazioni indispensabili per perseguire una

finalità di tutela della salute o dell'incolumità fisica dell'interessato;

b) anche senza il consenso dell'interessato e previa autorizzazione del Garante se la finalità di cui alla lettera a) riguarda un terzo o la collettività.

Il consenso può essere definito come un "contratto" tra l'interessato e l'Azienda, dove vengono stabiliti le modalità del trattamento e l'ambito di comunicazione dei dati ai quali il personale dell'Azienda deve attenersi.
Per essere valido, il consenso deve essere preceduto da una corretta informazione al paziente. L'ottenimento del consenso è **obbligatorio** per poter trattare i dati personali/sensibili del paziente per le finalità di cura.
Non esistono eccezioni a tale regola, infatti, anche quando ci si trova in una delle seguenti situazioni: emergenza sanitaria, impossibilità fisica, incapacità di agire o incapacità di intendere o di volere dell'interessato ecc., **il consenso deve essere comunque acquisito**, senza ritardo, successivamente alla erogazione della prestazione sanitaria, o può essere manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato.

È diritto dell'interessato rifiutare il consenso per i trattamenti che hanno finalità diverse da quelle indicate nell'informativa ed eccedenti e non pertinenti rispetto alle finalità della raccolta.
Per l'acquisizione del consenso l'ASST adotta apposita seguente modulistica:

Il consenso può essere acquisito secondo differenti modalità a seconda che si tratti di paziente degente o ambulatoriale.

Raccolta del consenso al trattamento dei dati personali e sensibili – (paziente - degente)
L'acquisizione del consenso scritto dell'interessato (paziente) da parte dell'ASST avviene al momento della prenotazione/accettazione amministrativa prima dell'erogazione della prestazione sanitaria.
L'acquisizione del consenso al trattamento dei dati, **con l'eccezione dei trattamenti urgenti**, da parte dell'ASST costituisce momento indispensabile e indifferibile e pertanto ha carattere d'obbligatorietà. L'eventuale rifiuto da parte dell'interessato di conferire in forma scritta il consenso al trattamento dei dati personali e sensibili, su apposito modulo, comporterà l'impossibilità da parte dell'Azienda di trattare i dati come dichiarato nella nota informativa.

- Consenso utente ricoverato (prericovero, ricovero ordinario, day hospital/day surgery)

Il personale che esegue l'accettazione amministrativa dell'interessato presentatosi per ciascun prericovero/ricovero, consegna il modulo di raccolta del consenso ad ogni accesso. Lo stesso personale chiede all'interessato l'autorizzazione affinché sia resa

gl

24

nota la sua presenza in ospedale e inserisce l'autorizzazione nella procedura informatica dedicata. In questo modo presso la portineria dell'Azienda sarà disponibile soltanto l'elenco degli interessati che desiderano ricevere visite. Il modulo diventa parte integrante di tutta la documentazione che costituisce la cartella clinica.

- Consenso utente ambulatoriale e di pronto soccorso

Il diretto interessato (paziente) presta il consenso orale al momento della prenotazione/accettazione amministrativa prima dell'erogazione della prestazione e l'Operatore sanitario annota l'avvenuto consenso nell'apposito campo del sistema informativo.

Sul modello cartaceo di prenotazione/accettazione comparirà la dicitura dell'avvenuta acquisizione del consenso.

Per i ricoveri d'urgenza (dei pazienti che passano per il Pronto Soccorso), gli adempimenti privacy (in particolare l'acquisizione del consenso scritto) saranno di competenza dei reparti.

- Consenso per il trattamento delle immagini:

Qualora fosse necessario acquisire una immagine che riprenda tutto il corpo del paziente, compreso il volto, il personale medico di reparto consegna all'interessato (paziente) il modulo contenente l'informativa e la raccolta del consenso al trattamento delle fotografie/immagini. Il modulo diventa parte integrante di tutta la documentazione che costituisce la cartella clinica.

Si rammenta che:

- nel caso di minorenni il consenso deve essere obbligatoriamente firmato da chi esercita legalmente la potestà. Dopo il raggiungimento della maggiore età, il consenso deve essere nuovamente richiesto e firmato dall'interessato.
- l'informativa ed il consenso al trattamento dei dati personali possono essere resi ed acquisiti successivamente alla prestazione, ma senza ritardo, in caso di **emergenza sanitaria o di igiene pubblica** per la quale la competente Autorità ha adottato un'ordinanza contingibile ed urgente, ai sensi dell'art..117 del D.Lgs. n° 112/1998.

- L'informativa ed il consenso possono essere resi ed acquisiti successivamente alla prestazione, ma senza ritardo, in caso di:

1. presenza di impedimenti fisici, incapacità di agire o incapacità di intendere o di volere dell'interessato quando non è possibile acquisire il consenso da chi esercita legalmente la potestà ovvero da un prossimo congiunto, da un familiare, da un convivente o in loro assenza dal responsabile della struttura presso cui dimora l'interessato;

2. rischio grave, imminente ed irreparabile per la salute dell'interessato;

3. prestazione medica che può essere pregiudicata dalla acquisizione preventiva del

25

consenso in termini di tempestività o efficacia.

I DIRITTI DELL'INTERESSATO

Il soggetto interessato, a cui si riferiscono i dati, esplica il diritto a:
- essere informato sull'esistenza o meno dei dati che lo riguardano;
- averne comunicazione in forma comprensibile;
- conoscere finalità e modalità di trattamento;
- essere informato sulla logica applicata al trattamento, ivi compreso l'utilizzo di strumenti elettronici e di particolari forme di elaborazione.

Diritto di accesso ai dati personali ed altri diritti (*art. 15 GDPR)*

L'interessato ha diritto di ottenere la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

a) le finalità del trattamento;
b) le categorie di dati personali in questione;
c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di Paesi terzi o organizzazioni internazionali;
d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali che lo riguardano o di opporsi al loro trattamento;
f) il diritto di proporre reclamo al Garante
g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
h) l'esistenza (eventuale) di un processo decisionale automatizzato, compresa la profilazione di cui all'art. 22, paragrafi 1 e 4 del GDPR e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Esercizio dei diritti e modalità di esercizio

L'interessato può esercitare i propri diritti mediante richiesta rivolta senza formalità al Titolare o al Responsabile, anche per il tramite di un incaricato, al quale (l'interessato) è fornito idoneo riscontro senza ritardo.
L'interessato può conferire delega o procura a persone fisiche, enti, associazioni o organismi o farsi assistere da persona di fiducia.
L'identità dell'interessato è verificata mediante esibizione di un documento di

riconoscimento.
La persona che agisce per conto dell'interessato esibisce o allega copia della procura, ovvero della delega sottoscritta in presenza di un incaricato o sottoscritta e presentata unitamente a copia fotostatica non autenticata di un documento di riconoscimento dell'interessato.
I diritti concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per motivi famigliari meritevoli di protezione.
Al fine di garantire l'esercizio dei propri diritti è disponibile sulla rete internet aziendale la relativa modulistica.

Sezione 4 - TRATTAMENTO DEI DATI PERSONALI IN AMBITO SANITARIO -

ALTRE MISURE PER IL RISPETTO DEI DIRITTI DELL'INTERESSATO

Gli organismi sanitari pubblici e privati devono adottare idonee misure per garantire nell'organizzazione delle prestazioni e dei servizi, il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati. La tutela della dignità della persona deve essere sempre garantita con particolare riguardo a fasce deboli (disabili, minori, anziani, soggetti che versano in condizioni di disagio o bisogno), a soggetti particolarmente vulnerabili (per disturbi psichici), a pazienti sottoposti a trattamenti medici invasivi e per i quali è doverosa una particolare attenzione.
Di seguito si riportano le misure che l'azienda è tenuta ad adottare per la tutela dell'interessato.

1. Chiamata del paziente presente in sala d'attesa

In tutti i locali in cui i pazienti sostano in attesa di una prestazione sanitaria o amministrativa (es. visite ambulatoriali, accettazione paziente, ritiro di referti diagnostici, ritiro di relazioni relative a prestazioni terapeutiche), gli stessi non devono essere chiamati per cognome e nome.
Il paziente deve essere chiamato prescindendo dall'individuazione nominativa (es. numero, ect.

2. Distanza di cortesia

L'Azienda ha predisposto dove necessario apposite distanze di cortesia nei casi in cui si effettua il trattamento dei dati sanitari (es. operazioni di sportello, accettazione paziente), nel rispetto dei canoni di confidenzialità e della riservatezza dell'interessato.

3. Riservatezza nei colloqui e nelle prestazioni sanitarie

1. All'interno della ASST, al di fuori di contesti tipicamente clinici (ad es. lungo i corridoi, bar, ascensori, cortile) non devono essere divulgate informazioni sanitarie in presenza di terzi non legittimati, anche solo attraverso commenti e/o considerazioni.
2. Il dialogo-colloquio tra personale dell'ASST (medici, infermieri, amministrativi ecc) e gli interessati, qualora abbia ad oggetto informazioni inerenti lo stato di salute

dell'interessato e qualora avvenga in spazi od in situazioni ove vi è la presenza d'altri soggetti oltre all'interessato (nelle stanze di degenza a più posti letto o nei punti ove vengono ritirati esami, referti ecc. o presso le accettazioni delle Unità Operative) deve essere improntato ad un criterio di prudenza.

3. Pertanto, è necessario adottare soluzioni tali da prevenire, durante i colloqui, l'indebita conoscenza da parte di terzi non legittimati di informazioni idonee a rivelare lo stato di salute.

4. A tale prudenza devono essere improntate tutte le condizioni usuali di colloquio tra operatori nell'esercizio della professione: discussione di casi clinici durante il giro visita, supervisione di casi in luoghi aperti all'utenza, consulenze specialistiche effettuate al letto di degenza, passaggi di consegne tra personale, comunicazioni di servizio effettuate mediante apparecchi telefonici portatili e non posizionati in luoghi protetti, informazioni fornite a frequentatori medici, consulenti ecc.

Stesso obbligo vale nel corso delle attività mediche e infermieristiche, in particolare quando queste avvengano in situazioni di promiscuità (es. ambienti multidisciplinari, stanza di degenza a più letti, ecc.). In questo caso devono essere adottati accorgimenti, anche provvisori, come ad esempio l'utilizzo di paraventi, che delimitano la visibilità dell'interessato. Inoltre in relazione alle prestazioni sanitarie effettuate alla presenza di **studenti autorizzati**, devono essere adottate specifiche cautele volte a limitare l'eventuale disagio dei pazienti, anche in relazione al grado di invasività del trattamento circoscrivendo, ad esempio, il numero degli studenti presenti e rispettando eventuali legittime volontà contrarie.

4. Rilascio di informazioni (telefono e fax)

Il Personale Amministrativo e Sanitario non è tenuto a rilasciare per telefono notizie sia sulla presenza che sullo stato di salute dell'interessato.

Questa regola generale subisce un' eccezione solo per i pazienti del Pronto Soccorso. Infatti, ove necessario, il Personale può dare correttamente notizia o conferma, anche telefonica, sul passaggio e/o sulla presenza di un paziente, solo a terzi legittimati di cui deve essere accertata l'identità anche avvalendosi di elementi desunti dall'interessato.

L'interessato, - se cosciente e capace - può decidere a quali soggetti (es. parenti, familiari, conviventi) possono essere comunicate tali informazioni.

Nel caso si debba procedere alla comunicazione tramite fax di dati sensibili all'interno delle aree di pertinenza dell'Ospedale, è opportuno che lo strumento fax sia collocato in un'area protetta e presidiata e che i Responsabili e gli Incaricati prestino attenzione alle fasi di invio e di ricevimento della documentazione, contenente dati personali sensibili.

5. Rilascio di informazioni sulla dislocazione del paziente nei reparti

L'interessato cosciente e capace deve essere informato e posto nelle condizioni di decidere che sia resa nota la propria presenza presso l'ASST, consentendo di fornire

l'informazione a chi ne faccia richiesta. Occorre altresì rispettare l'eventuale sua richiesta a che la presenza nella struttura sanitaria non sia resa nota. Tale autorizzazione è espressamente richiesta sul modulo di consenso per il paziente ricoverato.
Pertanto, il personale addetto all' accettazione amministrativa deve inserire nel sistema informativo l'indicazione relativa alla autorizzazione/non autorizzazione a che sia resa nota la presenza in Ospedale. Solo in questo modo nell'elenco presente in portineria compariranno i nominativi dei degenti che hanno autorizzato "che sia resa nota la presenza in questo Ospedale, consentendo di fornire l'informazione a chi ne faccia richiesta".
Questo genere di informazioni riguarda la sola presenza nel reparto e non informazioni sullo stato di salute; infatti, il personale della portineria può dare notizie relative alla sola presenza del paziente ricoverato presso l'Azienda, previa autorizzazione dell'interessato.

6. *Riservatezza dei dati e delle informazioni*

Non è ammessa l'affissione di liste di pazienti in attesa di ricovero o già ricoverati, elenchi di pazienti che accedono agli Ambulatori, programmi sanitari in locali aperti al pubblico o in cui il pubblico può avere accesso, con o senza la descrizione della patologia sofferta.
Non devono essere resi visibili ad estranei documenti sulle condizioni cliniche dell'interessato, quali cartelle cliniche, cartelle infermieristiche, cartelle riabilitative, referti, liste operatorie, certificazioni o altra documentazione sanitaria lasciata incustodita in luoghi diversi da quelli previsti (es. su carrelli posti in corridoi, sopra le scrivanie ecc.). I fogli riportanti risultati di parametri clinici (es. curve termografiche poste sul letto di degenza) non devono essere consultabili da parte di persone non autorizzate (esempio oscurando tali dati).

7. *Correlazione fra paziente e reparto o struttura*

Per prevenire che soggetti estranei possano evincere in modo esplicito informazioni sullo stato di salute del paziente attraverso la semplice correlazione tra la sua identità e l'indicazione del reparto/ambulatorio/servizio presso cui si è recato o è stato ricoverato, è necessario che qualsiasi documento sanitario e/o amministrativo prodotto sia consegnato o inviato all'interessato su carta intestata dell'ASST e in busta chiusa, sulla quale però non deve essere riportata l'intestazione del reparto/ambulatorio/servizio. Tali cautele devono essere estese anche ad eventuali certificazioni richieste per fini amministrativi (es. giustificare un'assenza del lavoro).

8. *Personale volontario e dei Servizi appaltati (ristorazione, pulizia, etc.)*

Il personale che presta attività di volontariato e gli incaricati delle Società che effettuano servizio presso i reparti devono attenersi a regole di condotta analoghe al

segreto professionale su tutte le informazioni di cui vengano a conoscenza durante l'espletamento dell'attività.

Particolare riservatezza e misure di garanzia per i pazienti affetti da HIV

I dati anagrafici relativi a persone sieropositive o affette dall'AIDS devono essere conservati separatamente da quelli sanitari. Inoltre, se questi ultimi sono contenuti in elenchi, registri e banche dati, devono essere trattati con tecniche di cifratura o sistemi che permettano di identificare gli interessati solo in caso di necessità.

La Legge n. 135 del 1990 sulla lotta all'AIDS, prevede, da un lato, che "nessuno può essere sottoposto, senza il suo consenso, ad analisi tendenti ad accertare l'infezione da HIV, salvo che per motivi di necessità clinica e nel proprio interesse" e, dall'altro "che la rilevazione statistica della infezione da HIV deve comunque essere effettuata con modalità che non consentano l'identificazione della persona".

Fermo restando che il medico è tenuto a raccogliere un'anamnesi dettagliata del paziente ed a illustrare a quest'ultimo l'importanza di tale raccolta di dati personali, l'interessato è comunque libero di scegliere, in modo informato e quindi consapevole - di non comunicare al medico alcune informazioni sanitarie che lo riguardano, ivi compresa la sua eventuale sieropositività, senza per ciò subire alcun pregiudizio sulla possibilità di usufruire delle prestazioni sanitarie richieste.

La raccolta di informazioni relative all'eventuale stato di sieropositività di ogni singolo paziente da parte degli esercenti le professioni sanitarie deve avvenire **in conformità ai principi di pertinenza e non eccedenza dei dati rispetto alle finalità del trattamento riconducibili alle specifiche attività di cura dell'interessato.**

Gli esercenti le professioni sanitarie, infatti, previo consenso informato del paziente- possono raccogliere l'informazione relativa all'eventuale presenza di un' infezione da HIV **solo qualora tale dato anamnestico sia ritenuto dagli stessi necessario in funzione del tipo di intervento sanitario o di piano terapeutico da eseguire sull'interessato;** resta fermo che quest'ultimo rimane libero di decidere in modo consapevole (e quindi informato) e responsabile di non comunicare al medico alcuni eventi sanitari che lo riguardano.

La raccolta delle informazioni sullo stato di sieropositività va ricondotta, quindi, ai principi di cui sopra, e non si può sicuramente ricondurre alla necessità di attivare specifiche misure di protezione per il personale sanitario, in quanto la normativa di settore prevede che, stante l'impossibilità di avere certezza sullo stato di sieropositività del paziente, le misure di protezione devono essere adottate nei confronti di ogni singolo assistito, a prescindere dalla conoscenza dello stato di sieropositività.

La Legge 5 giugno 1990, n. 135 (Programma di interventi urgenti per la prevenzione e la lotta contro l'AIDS), infatti, ha previsto specifiche disposizioni per la protezione del contagio professionale da HIV nelle strutture sanitarie ed assistenziali pubbliche e private, attuate con decreto del Ministro della sanità del 28 settembre 1990.

Più precisamente, il predetto decreto, nel considerare impossibile *"identificare con*

certezza tutti i pazienti con infezione da HIV", ha previsto che le *"precauzioni finalizzate alla protezione dal contagio"* debbano essere prestate *"nei confronti della generalità delle persone assistite"* (cfr. premesse del citato decreto).

Ritiro dei referti diagnostici e documentazione sanitaria.

Tutti i referti/lettere di dimissioni ed in generale la documentazione sanitaria deve essere consegnata in busta chiusa al diretto interessato. I documenti predetti possono essere ritirati, in busta chiusa, anche da persona diversa dal diretto interessato purché munita di delega scritta e firmata dallo stesso e di documenti di identità validi del delegante e del delegato. La persona addetta alla consegna dei referti si accerta dell'identità del delegato prima di consegnare i referti.
La comunicazione di risultati di accertamenti diagnostici diretti o indiretti per infezione da HIV può essere data esclusivamente alla persona cui tali esami sono riferiti (art. 5 comma 4, legge 135/1990)

Modalità di trasporto interno all'ASST della documentazione cartacea

Quando le cartelle cliniche, liste operatorie, ed altra documentazione contenente dati personali e sensibili deve essere trasportata all'interno dell'Ospedale, è necessario utilizzare buste chiuse, cassette munite di serratura o contenitori equipollenti, al fine di impedire un accesso non autorizzato a tale documentazione da parte del personale che esegue la movimentazione.
Il personale addetto al trasporto della documentazione deve limitarsi alla sola movimentazione, non avendo l'autorizzazione all'accesso e alla consultazione.

USO DELLE PERIFERICHE

Telefono

Il telefono deve essere utilizzato limitando al minimo il rischio che i dati possano essere indebitamente riferiti a soggetti non legittimati.
La procedura da applicare prevede pertanto che le informazioni relative allo stato di salute dell'Interessato non siano date via telefono, salva l'ipotesi in cui il paziente sia stato informato specificamente su questa possibile modalità di trasmissione ed abbia espresso il proprio consenso.
Questa procedura si applica anche nell'ipotesi in cui sia data conferma via telefono di un esame clinico prenotato: anche in tal caso è necessario informare e acquisire il consenso.

Fotocopiatrice

La fotocopiatrice deve essere ubicata in una zona controllata dal personale autorizzato (ad esempio guardiola infermieri) onde limitare il rischio che i documenti (in originale o fotocopia) possano essere oggetto di accesso non autorizzato.

Quale ulteriore accorgimento è opportuno rispettare (ed eventualmente affiggere) il seguente regolamento d'uso:

- l'uso della fotocopiatrice è consentito ai soli soggetti autorizzati;
- le operazioni di fotocopiatura dei documenti contenenti dati personali sono svolte dagli incaricati privacy autorizzati nel rispetto del GDPR;
- l'incaricato privacy non può utilizzare carta riciclata recante, sul retro del foglio, dati personali;
- l'incaricato privacy non può lasciare incustodita la documentazione durante lo svolgimento delle operazioni di fotocopiatura;
- l'incaricato privacy pone nel cestino una fotocopia recante dati personali solo previa adeguata distruzione della stessa;
- al termine delle medesime operazioni, l'incaricato privacy deve provvedere al ritiro tempestivo degli originali e delle copie dalla fotocopiatrice.

Fax

Il fax non deve essere utilizzato per trasmettere all'Interessato dati sul suo stato di salute (ad esempio i referti degli esami effettuati) in quanto tali dati possono essere comunicati all'Interessato solo tramite un medico designato dallo stesso o dall'Ospedale.
In casi eccezionali giustificati dall'urgenza clinica, è possibile trasmettere referti nel rispetto della seguente procedura:

- invio interno (alle altre strutture aziendali): deve essere utilizzato l'elenco predisposto dalla Direzione che ha individuato i fax abilitati e ubicati in area protetta e presidiata;
- invio esterno (a enti esterni all'Azienda): deve preventivamente essere chiesto al preposto di indicare per iscritto il numero di fax al quale inviare il documento.

Come la fotocopiatrice, anche il fax deve essere collocato in una zona non liberamente accessibile al pubblico onde evitare che informazioni riservate possano essere indebitamente lette da chi non è autorizzato.
Se ciò non è possibile, il fax deve essere perlomeno controllabile "a vista" dal personale di reparto .

I fax in "uscita" devono recare in calce una formula del seguente tenore: "*Questo documento-fax è riservato. In caso di erronea ricezione si prega di distruggere il documento e di contattare il n.* _____").
Qualora si tratti di un numero faxato per la prima volta, è opportuno accertarsi con una preventiva telefonata in ordine al fatto che il documento sarà ritirato da un soggetto autorizzato.
I fax in "entrata" devono essere ritirati il prima possibile dagli Incaricati onde limitare al minimo il periodo di incustodita e quindi pericolosa giacenza degli stessi.

Sezione 5 - ALTRE DISPOSIZIONI

Comunicazione di dati dell'interessato

In merito all'aspetto delicatissimo della comunicazione delle informazioni sullo stato di salute, si considerano due importanti momenti:

1. chi può comunicare,
2. a chi possono essere comunicati i dati.

In relazione al primo punto, si vuole evitare che il soggetto interessato (paziente) abbia un danno dall'apprendere notizie che riguardano la sua salute: o perché non in grado di valutare correttamente la terminologia diagnostica usata dal medico, o perché affetto da patologie non compatibili con il tipo di informazione che deve essere comunicata (si pensi ai soggetti cardiopatici). La soluzione adottata dall'abrogato Codice (alla quale ci si riferisce in assenza di diverse disposizioni sul punto) è quella di permettere che l'informazione al paziente avvenga solo attraverso l'intermediazione del medico curante dell'ASST, se designato direttamente dall'interessato: questo per rendere possibile usufruire il supporto di consulenza che solo soggetti preparati e di fiducia del paziente possono fornire.
Per quanto riguarda il secondo punto, la richiamata norma stabilisce che il medico può comunicare informazioni sullo stato di salute esclusivamente all'interessato o a persone da lui autorizzate. I nominativi delle persone legittimate, ivi incluso il nominativo del medico curante, devono essere desunti dal modulo del consenso al trattamento dei dati paziente ricoverato, ove sono stati identificati dall'interessato.

Trattamento dei dati genetici

A partire dal 1 aprile 2007, medici, in particolare genetisti, organismi sanitari, laboratori di genetica, istituti di ricerca, farmacisti dovranno rispettare le prescrizioni contenute nell'autorizzazione generale del Garante per la privacy, che fissa, per la prima volta in maniera specifica e sistematica i principi, i limiti e le garanzie in base ai quali dovranno d'ora in poi essere trattati questi delicatissimi dati personali.

Il 24 giugno del 2011 è stata aggiornata la prima autorizzazione e rinnovata ogni 18 mesi. In attesa di chiarimenti sul trattamento dei dati genetici in conseguenza della entrata in vigore del GDPR, ci si richiama comunque alle regole dettate dal Garante nelle sue autorizzazioni.
Di seguito vengono indicate le regole da seguire per il trattamento dei dati genetici:
Modalità di raccolta e trattamento: devono essere predisposte misure specifiche per accertare in modo univoco l'identità del soggetto a cui viene prelevato il materiale genetico; i dati identificativi devono essere tenuti separati già al momento della raccolta.
Accertare l'identità del soggetto con un valido documento di riconoscimento.
Informativa: è necessario informare l'interessato sugli scopi perseguiti, sui risultati conseguibili, sul periodo di conservazione dei dati e dei campioni biologici. Al momento di eseguire un esame di tipo genetico rendere all'interessato l'informativa redatta dall'Azienda.
Consenso: è obbligatorio il consenso scritto dell'interessato per trattare i dati genetici e utilizzare i campioni biologici; il consenso è revocabile in ogni momento. Dopo avere reso l'informativa all'interessato, acquisire il consenso scritto con il modulo redatto dall'azienda.
Nascituri: il consenso per i test genetici relativi ai nascituri è espresso dalla madre e se l'esame può rivelare l'insorgenza di patologie del padre, anche da quest'ultimo.
Misure di sicurezza: i dati genetici e i campioni biologici contenuti nelle banche dati devono essere trattati con tecniche di cifratura; i dati possono essere consultati solo mediante rigorosi sistemi di autenticazione; la trasmissione dei dati in formato elettronico deve avvenire tramite posta elettronica certificata. L' acceso ai locali è controllato mediante incaricati della vigilanza o strumenti elettronici che prevedano specifiche procedure di identificazione anche mediante dispositivi biometrici. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate; il trasporto dei dati genetici all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti.
Conservazione: i campioni biologici e i dati genetici non possono essere conservati per un periodo di tempo superiore a quello strettamente necessario per perseguire gli scopi per i quali sono stati raccolti e utilizzati.
Diffusione: i dati genetici non possono essere diffusi. I risultati delle ricerche possono essere comunicati solo in forma aggregata.
E' **vietato al datore di lavoro e alle assicurazioni di usare dati genetici.**

Cartella clinica e diritto di accesso

La cartella clinica deve essere redatta in modo chiaro e comprensibile per assicurare la leggibilità formale e sostanziale delle informazioni in essa contenute.
La cartella deve inoltre riportare in modo separato i dati del paziente da quelli relativi

a soggetti terzi (compreso, ad esempio, il nascituro).

La persona alla quale i dati della cartella si riferiscono ha diritto di disporre del suo contenuto, sia nel corso della degenza (a cartella cosiddetta aperta) sia dopo la sua dimissione.
Per definire le modalità e i limiti dell'accesso alla cartella clinica, occorre raccordare una serie di disposizioni normative, derivanti dalla L. 241/90, dal D.Lgs 196/2003, avuto altresì riguardo alle previsioni del codice penale in tema di tutela del segreto professionale (art. 622) e del segreto d'ufficio (art. 326).

Sulla possibile conflittualità tra la normativa relativa al "diritto di accesso" (disciplinata dalla Legge 241/1990) ed il "diritto di accesso ai dati personali" si è pronunciato in più occasioni il Garante per la protezione dei dati personali, precisando che il bilanciamento è frutto di una continua ricerca di un giusto punto di equilibrio tra due interessi meritevoli, entrambi, di tutela.
In tema di documentazione sanitaria, è opportuno sottolineare che, laddove il trattamento concerne dati idonei a rivelare lo stato di salute o la vita sessuale, la L. 241/1990 rimanda espressamente all'articolo 60 del Codice Privacy, che consente il trattamento se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi è di rango almeno pari ai diritti dell'interessato.
A tal proposito il Garante è intervenuto nel 2003, per chiarire come il destinatario della richiesta deve valutare il **"rango"** del diritto del terzo e giustificare, o meno, l'accesso o la comunicazione di dati: il Garante ha sottolineato che il parametro di raffronto non è "il diritto di azione e difesa", quanto il diritto sottostante che il terzo intende far valere sulla base del materiale documentale che chiede di conoscere, che può essere ritenuto di "pari rango" rispetto a quello dell'interessato solo se fa parte della categoria dei diritti della personalità o è compreso tra altri diritti o libertà fondamentali ed inviolabili.

In sintesi, hanno diritto alla consultazione e ottenere copia della cartella, in toto o in parte, oltre che al rilascio di estratti della stessa, anche durante il tempo in cui la cartella è aperta:

- **la persona assistita (interessato),** a cui la documentazione si riferisce, in via diretta, se maggiorenne e capace di intendere e volere;
- per il tramite degli **esercenti la potestà o la tutela, se minorenne** oppure di **maggiore età ma incapace di intendere o volere o per il tramite dell'amministratore di sostegno,** se tale compito rientra tra quelli assegnatigli dal giudice tutelare;
- **persone delegate dall'interessato.**

In ipotesi di decesso dell'interessato, hanno titolo, ciascuno per proprio conto:

- **gli eredi legittimi** (il coniuge, i figli legittimi, i figli naturali e, in mancanza dei predetti, gli ascendenti legittimi e i collaterali se concorrono come legittimari);
- **gli eredi testamentari** che provino la loro posizione con dichiarazione sostitutiva di atto di notorietà, corredata da copia di documento di identità o di riconoscimento valido.

  Quando tra le persone sopra indicate intervenga dissenso, la decisione va rimessa all'autorità giudiziaria competente; è da riconoscersi un diritto di accesso al parente del defunto interessato a scopo di tutela della propria salute.

  La richiesta deve essere specificatamente motivata e la legittimazione dell'istante deve essere comprovata mediante dichiarazione sostitutiva di atto di identità o di riconoscimento di notorietà ai sensi dell'art. 47 del DPR n° 445/2000, corredata da copia di documento di riconoscimento valido.

  Va rispettata in ogni caso la volontà del defunto quando risulti espressa in forma scritta.

L'accesso può essere consentito inoltre:

- **al minore emancipato**, ai sensi dell'art. 390 cc, sulla base di idonea certificazione o dichiarazione sostitutiva;

- **la persona che non sia stata riconosciuta dai genitori naturali** può chiedere l'accesso ai propri documenti sempre che le generalità riportate su questi ultimi corrispondano a quelle del richiedente.

Altri soggetti a cui consentire l'accesso sono:

- **il medico curante o le strutture sanitarie pubbliche o private**, esclusivamente per finalità istituzionali attinenti alla tutela della salute dell'interessato, previo consenso di quest'ultimo;
- **l'INAIL** per le finalità proprie;
- **l'Autorità Giudiziaria**, in via autonoma o con delega alla Polizia Giudiziaria o ai consulenti tecnici da essa nominati.

Il responsabile del rilascio deve consegnare i documenti richiesti anche in originale se così è ordinato dall'Autorità giudiziaria (v. art. 258 cpp); in tal caso a quest'ultima dovrà essere chiesta autorizzazione a ottenere una copia per esigenze di archivio, con divieto di estrazione di copie ulteriori, per il cui rilascio si dovrà acquisire specifico nulla osta.

La consultazione per scopi storici di documenti con dati personali è assoggettata alle disposizioni del codice di deontologia e di buona condotta e può avvenire liberamente decorsi 70 anni, con l'eccezione della documentazione sanitaria inerente

alle madri che non abbiano riconosciuto il loro neonato, per le quali vale il termine di 100 anni.
Prima dei 70 anni, l'accesso agli archivi sanitari, per motivi storici, richiede l'autorizzazione della struttura che ne è responsabile

L'accesso alla documentazione sanitaria per **studi epidemiologici** è disciplinato dall'art.110 del Cod. priv. secondo il quale, al di fuori di ricerche previste da leggi o rientranti nell'ambito di programmi di ricerca biomedica o sanitaria previsti dalla normativa regolante il SSN, **occorre il consenso dell'interessato.**
In situazioni particolari, quando non sia possibile acquisire il consenso degli interessati, si può sottoporre il programma di studio alla valutazione del comitato etico territorialmente competente e, in caso di giudizio favorevole, richiedere poi l'autorizzazione del Garante per la protezione dei dati.

Trattamento dei dati personali effettuato per scopi di ricerca scientifica.
In attesa di specifiche sul trattamento dei dati personali effettuato per scopi di ricerca scientifica, in conseguenza della entrata in vigore di GDPR, si richiama, in via generale, la disposizione del Regolamento che richiede al titolare di adottare le misure di sicurezza tecniche e di tipo organizzativo dirette ad assicurare la minimizzazione dei dati, anche attraverso la pseudonimizzazione degli stessi, che non consente di ricondurre l'informazione al singolo interessato.
Come espresso nel considerando n. 157 del Regolamento, i dati personali possono essere trattati per finalità di ricerca scientifica, fatta salva l'adozione di condizioni e garanzie adeguate.

In attesa di più precise indicazioni da parte del legislatore, si reputa comunque opportuno inserire nell'informativa che il trattamento dei dati, laddove ne ricorrano le condizioni di legge, e con le modalità specificate dal legislatore (es. in forma anonima) può essere realizzato anche per scopi di ricerca scientifica.

Resta fermo l'obbligo di raccogliere il consenso al trattamento dei dati degli interessati inclusi nella ricerca in tutti i casi in cui, nel corso dello studio, sia possibile rendere loro un'adeguata informativa e, in particolare, laddove questi si rivolgano al centro di cura, anche per visite di controllo.

Misure di sicurezza: criteri tecnici ed organizzativi per la protezione dei locali e dei documenti cartacei.

Obblighi di sicurezza (art. 32 GDPR)

I dati personali, oggetto di trattamento, sono custoditi e controllati, anche in relazione

alle conoscenze acquisite in base al progresso tecnologico, in base alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non conforme alle finalità della raccolta.
Di seguito si riportano le misure minime di sicurezza criteri tecnici ed organizzativi per la protezione dei locali e dei documenti cartacei.

Il Responsabile del trattamento individua nella propria organizzazione luoghi sicuri, stanze e/o uffici, in cui vengono svolte le operazioni di trattamento aventi ad oggetto i dati sensibili, nonché locali e stanze destinate alla loro conservazione/archiviazione. L'accesso a tali locali deve essere consentito al solo personale autorizzato per l'espletamento della propria attività lavorativa ed esclusivamente negli orari di lavoro; ove risulta possibile, devono essere utilizzati anche schedari, armadi, cassetti e quant'altro dotati di serratura. Tali locali devono sempre essere presidiati dal personale autorizzato, e se non presidiati, i documenti devono essere collocati in armadi/schedari chiudibili o nella stessa stanza chiudibile. Sulle porte di ingresso di tali locali devono essere posizionati cartelli che vietano l'ingresso ai soggetti non autorizzati al trattamento dei dati.
I documenti oggetto di trattamento sono affidati soltanto a **soggetti appositamente autorizzati (Responsabili ed incaricati del trattamento)** e nel rispetto del proprio ambito di trattamento.
I documenti contenenti dati personali prelevati dagli archivi per l'attività quotidiana, devono essere ivi collocati al termine della giornata.

Durante il trattamento: e per tutto il periodo che i documenti sono all'esterno del luogo sicuro, l'Incaricato non deve mai perderli di vista, adempiendo ad un preciso obbligo di custodia e controllo dei documenti stessi, per evitare che ad essi accedano persone prive di autorizzazione; in particolare non devono rimanere incustoditi su scrivanie o tavoli di lavoro.
In caso di interruzione, anche temporanea, del lavoro verificare che i dati trattati non siano accessibili a terzi non autorizzati.
Concluso il trattamento, l'Incaricato deve controllare che i documenti siano sempre completi, verificando sia il numero dei fogli che l'integrità del contenuto e deve collocarli nelle stanze presidiate destinate all'archiviazione.
Inoltre:

- in occasione della **trasmissione dei documenti sia all'interno che all'esterno dell'Azienda** devono essere adottati tutti gli accorgimenti necessari e idonei onde evitare che le informazioni riservate possano essere lette sia pure accidentalmente da chi non è autorizzato (ad esempio trasporto mediante cartelle chiuse);
- in occasione della trasmissione dei documenti agli interessati, gli stessi devono

essere risposti **in busta chiusa**, priva all'esterno di informazioni sensibili, da consegnarsi direttamente all'Interessato o al terzo delegato per iscritto;

- i documenti recanti **dati genetici** possono essere trasportati all'esterno dai locali riservati al loro trattamento soltanto mediante **contenitori muniti di serratura** o altri dispositivi equipollenti
- i documenti **non devono essere riciclati** (ad esempio per carta da minuta o per le fotocopie) onde evitare il rischio che gli stessi possano essere letti da chi non è autorizzato;
- è vietata la fotocopiatura e/o duplicazione di documenti originali senza la preventiva autorizzazione del responsabile.
- i documenti contenenti dati personali e sensibili **devono essere eliminati** utilizzando gli appositi apparecchi "distruggi documenti" o, in assenza, sminuzzati in modo da non essere più ricomponibili;
- i documenti possono essere affissi in stanze ad accesso selezionato a condizione che siano posizionati in modo tale da **evitare che le informazioni possano essere lette sia pure accidentalmente da chi non è autorizzato** (ad esempio, sulla parte interna dell'anta di una armadio, in un cassetto, eccetera).
- è vietata la diffusione dei dati;
- è vietata la comunicazione dei dati senza la preventiva autorizzazione del Responsabile;

Archivi cartacei correnti

L'archivio corrente comprende i documenti attualmente in uso nei vari servizi e reparti. La gestione degli archivi cartacei correnti si ascrive alla competenza e responsabilità del Responsabile del trattamento. Lo stesso individua le tipologie dei documenti contenenti i dati sensibili e giudiziari ed i dipendenti incaricati dei relativi trattamenti. Il Responsabile deve assicurare che la documentazione venga custodita in locali ad accesso selezionato e presidiato. In mancanza, in armadi dotati di serratura, le cui chiavi dovranno essere conservate in modo appropriato.

Per quanto riguarda il trattamento di tutta la documentazione sanitaria all'interno delle varie Unità Operative, in particolare la cartella clinica, questa viene gestita e conservata dal personale sanitario dell'UO fino alla dimissione del paziente; successivamente è inviata all'archivio clinico per la conservazione. La cartella clinica e tutta la documentazione sanitaria del paziente deve essere conservata all'interno di locali il cui accesso è consentito esclusivamente agli Incaricati del trattamento.

I locali destinati all'archiviazione devono essere adeguatamente presidiati.

Archivi cartacei storici

L'archivio storico comprende i documenti che hanno esaurito il loro ciclo di trattamento (es. cartelle cliniche dimessi, fascicoli del personale in pensione, pratiche amministrativa concluse ect...)

L'accesso alla documentazione di tali archivi non è pubblica.
La consultazione è consentita solo negli orari di apertura e potrà avvenire esclusivamente da parte del personale autorizzato in seguito a richiesta scritta e motivata. L'incaricato dell'archivio deve annotare su apposito registro gli estremi di ogni consultazione, precisando la data, la struttura richiedente, l'identità del soggetto che procede alla consultazione, l'oggetto della consultazione, le operazioni effettuate.
I documenti contenenti dati sensibili o giudiziari devono essere conservati secondo modalità che precludano la visione, in occasione della consultazione di documenti di altro genere, mediante creazione di sottofascicoli.
La selezione e lo scarto della documentazione avviene nel rispetto delle prescrizioni normative vigenti.

Le persone ammesse, a qualsiasi titolo, ad accedere agli archivi contenenti dati sensibili e/o giudiziari fuori orario di lavoro, devono essere autorizzate, identificate e registrate su apposito registro.

Sezione 6 – VALUTAZIONE DI IMPATTO, RESPONSABILE DELLA PROTEZIONE DEI DATI, REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO, SANZIONI

VALUTAZIONE DI IMPATTO

In considerazione della natura dei dati trattati l'ASST è tenuta ad effettuare la valutazione di impatto di cui all'articolo 35 del GDPR

RESPONSABILE DELLA PROTEZIONE DEI DATI

Ai sensi degli articoli 37-38-39 del GDPR, il titolare del trattamento designa un responsabile della protezione dei dati, che deve essere adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.

Il responsabile della protezione dei dati è incaricato dei seguenti compiti:
- informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni del legislatore europeo e nazionale;
- sorvegliare l'osservanza del regolamento, di altre disposizioni del legislatore europeo e nazionale relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo,
- fornire, se richiesto, un parere in merito alla valutazione di impatto sulla

protezione dei dati e sorvegliarne lo svolgimento
- cooperare con l'autorità di controllo (Garante);
- fungere da punto di contatto per l'autorità di controllo (Garante) per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del GDPR ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

IL REGISTRO DELLE ATTIVITA' DI TRATTAMENTO

Ai sensi dell'articolo 30 del GDPR è obbligatoria la tenuta del registro delle attività di trattamento, il quale deve contenere le seguenti informazioni:

- il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
- le finalità del trattamento;
- una descrizione delle categorie di interessati e delle categorie di dati personali;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49 GDPR, la documentazione delle garanzie adeguate;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1 GDPR.

Su richiesta, il registro deve essere messo a disposizione del Garante.

SANZIONI

per il regime sanzionatorio correlato alla violazione delle disposizioni in tema di tutela dei dati personali, si rinvia al contenuto degli articoli 83 e 84 del GDPR