ALLEGATO B
INDIVIDUAZIONE E NOMINA DELLE PERSONE AUTORIZZATE AL TRATTAMENTO DEI DATI PERSONALI

ai sensi del Regolamento Generale sulla protezione dei dati personali 2016/679 e del D. Lgs. 196/2003 (Codice Privacy) così come novellato dal D. Lgs. 101/2018

L'Azienda Sanitaria Locale ASM Matera, nella persona del suo legale rappresentante, ha previsto, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, chele persone le quali operano sotto la propria diretta autorità siano Autorizzate al Trattamento dei dati personali.

PREMESSO CHE

- 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 (di seguito, "Regolamento"), fissa le modalità da adottare e individua i soggetti che, in relazione all'attività svolta, sono tenuti agli adempimenti previsti dal Regolamento;
- l'art. 4 del Regolamento afferma che 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". Per "trattamento dei dati personali" si intende "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";
- l'art. 29 del Regolamento prevede che "il Responsabile del Trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento";
- l'art. 32, paragrafo 4, del Regolamento prevede che "il Titolare del Trattamento e il Responsabile del Trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso, salvo che lo richieda il diritto dell'Unione o degli Stati membri";
- in base all'art. 2-quaterdecies, comma 2, del D.lgs. n.196/2003 (Codice Privacy) ì come novellato dal D.lgs. n.101/2018, e in virtù del principio di "Accountability" (Responsabilizzazione e capacità di dimostrare che si adempie) . Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta".

Tutto ciò premesso

INDIVIDUA E NOMINA "AUTORIZZATI AL TRATTAMENTO DATI"

Tutti coloro i quali a qualsiasi titolo trattano dati all'interno di ciascuna Struttura/Ufficio sotto la diretta autorità del Titolare e/o dei Designati del trattamento

La persona è autorizzata a trattare i dati personali di cui viene a conoscenza per la Sua funzione/attività, nell'ambito dei trattamenti censiti nel Registro dei Trattamenti.

Le presenti istruzioni sono relative a tutte le operazioni di trattamento dei dati personali che siano strettamente necessarie per adempiere ai compiti assegnati in relazione alle attività svolte, compresa l'eventuale attività attuata in regime di libera professione intramuraria e intramuraria "allargata", e di quant'altro definito di volta in volta ed in modo specifico dal Titolare o dal Designato al trattamento.

ISTRUZIONI

Nell'effettuare il trattamento dei dati l'autorizzato dovrà scrupolosamente attenersi alle norme di legge, ai regolamenti, alle procedure aziendali, alle circolari interne, agli ordini di servizio emanati in materia e alle seguenti istruzioni di carattere generale:

- Trattare i dati in modo lecito e corretto;
- Adottare idonee misure per garantire, nell'organizzazione delle prestazioni e dei servizi, il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale, fermo restando quanto previsto dalle leggi e dai regolamenti in materia di modalità di trattamento delle categorie particolari di dati,

  in particolare:

  1) soluzioni volte a rispettare, in relazione a prestazioni sanitarie o ad adempimenti amministrativi preceduti da un periodo di attesa all'interno di strutture, un ordine di precedenza e di chiamata degli interessati prescindendo dalla loro individuazione nominativa;

  2) l'istituzione di appropriate distanze di cortesia, tenendo conto dell'eventuale uso di apparati vocali o di barriere;

  3) soluzioni tali da prevenire, durante colloqui, l'indebita conoscenza da parte di terzi di informazioni idonee a rivelare lo stato di salute;

  4) cautele volte ad evitare che le prestazioni sanitarie, ivi compresa l'eventuale documentazione di anamnesi, avvenga in situazioni di promiscuità derivanti dalle modalità o dai locali prescelti;

  5) il rispetto della dignità dell'interessato in occasione della prestazione medica e in ogni operazione di trattamento dei dati;

  6) la previsione di opportuni accorgimenti volti ad assicurare che, ove necessario, possa essere data correttamente notizia o conferma anche telefonica, ai soli terzi legittimati, di una prestazione di pronto soccorso;

  7) la formale previsione, in conformità agli ordinamenti interni delle strutture ospedaliere e territoriali, di adeguate modalità per informare i terzi legittimati in occasione di visite sulla dislocazione degli interessati nell'ambito dei reparti, informandone previamente gli interessati e rispettando eventuali loro contrarie manifestazioni legittime di volontà;

- Trattare le categorie particolari di dati (ex dati sensibili), contenuti in elenchi, registri o banche di dati tenuti con l'ausilio di mezzi elettronici o comunque automatizzati solo se forniti dall'azienda, e quindi, ove possibile, con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altri sistemi, che permettano di identificare gli interessati solo in caso di necessità;
- Raccogliere e registrare i dati unicamente per gli scopi inerenti l'attività svolta e per finalità determinate, esplicite e legittime;
- Verificare ove possibile, che i dati siano esatti e, se necessario, aggiornarli;
- Verificare che i dati siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti o successivamente trattati, secondo le indicazioni ricevute dal Titolare o dal Designato;
- Non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza esplicita autorizzazione del Titolare o del Designato;
- Conservare i dati in una forma che consenta l'identificazione degli interessati per un periodo di tempo non superiore al conseguimento delle finalità per le quali sono trattati;
- Evitare di creare banche dati nuove senza espressa autorizzazione del Titolare o del Designato del trattamento;
- Mantenere la massima riservatezza sui dati trattati;
- Osservare scrupolosamente le disposizioni organizzative e operative impartite dal Titolare o dal Designato;
- Accedere ai soli dati personali la cui conoscenza sia strettamente necessaria in relazione e per l'adempimento delle mansioni e dei compiti assegnati;
- Accedere, per esigenze di servizio, esclusivamente alle banche dati informatiche del proprio Servizio/Ufficio a cui è stato autorizzato dal Titolare o dal Designato;
- Non comunicare a terzi o diffondere, con o senza strumenti elettronici, le notizie, le informazioni o i dati appresi in relazione a fatti e circostanze di cui sia venuto a conoscenza nella propria qualità di soggetto autorizzato;
- Non comunicare e diffondere i dati personali provenienti da banche dati aziendali, in assenza dell'autorizzazione del Titolare o del Designato del trattamento;
- Richiedere preventivamente l'autorizzazione al Designato ogni qualvolta si renda necessaria la comunicazione all'esterno dei dati oggetto del trattamento;
- Osservare tutte le misure di protezione e sicurezza, già in atto o successivamente disposte, atte ad evitare rischi di distruzione, perdita, accesso non autorizzato, o trattamento non consentito dei dati personali, attenendosi inoltre, nel trattamento dei dati con o senza l'ausilio di strumenti elettronici, alle ulteriori particolareggiate istruzioni a tal fine impartite dal Designato;
- Prestare attenzione al fenomeno di "social engineering" (ingegneria sociale), utilizzato per carpire informazioni in maniera illecita. Un esempio tipico è il "phishing", ossia una pratica in cui si viene indotti a comunicare informazioni ed effettuare operazioni a seguito di e-mail o "profili fake" (spoofing). Pertanto a seguito di comunicazioni (email, sms, etc.) di dubbia provenienza e sospette si raccomanda di non inserire e/o inviare credenziali, non scaricare file/documenti e non aprire i link;
- Passare le consegne in modo preciso e dettagliato nel caso di trasferimento dell'attività svolta ad altro soggetto;

- Informare tempestivamente, non oltre le 24 ore, il Designato qualora si verifichi qualsiasi evento che possa compromettere la sicurezza dei dati personali: (anomalie, furti, perdite accidentali di dati) al fine di attivare, nel caso sia riscontrato un rischio grave per i diritti e le libertà delle persone fisiche, la procedura aziendale in caso di violazione di dati personali (data breach), pubblicata sul sito internet nell'area pubblica Sezione Privacy; rispettare le disposizioni contenute nel Codice di Comportamento Aziendale e Codice Etico disponibile sul sito istituzionale nella sezione Amministrazione trasparente | Disposizioni Generali | Atti generali.

L'autorizzato è altresì tenuto a seguire gli eventi formativi aziendali in materia di protezione dei dati personali (FAD e corsi in aula) come da piano di formazione della ASL.

Fanno parte integrante di queste istruzioni le politiche aziendali aziendale e le procedure in materia privacy e sicurezza tra cui "Procedura in caso di violazione di dati personali (Data Breach)", "Procedura per la gestione dei diritti dell'Interessato" e le istruzioni operative fornite dalla ASL tramite disposizioni e circolari interne pubblicate sul sito internet dell'ASL di Matera nella Sezione Privacy. Ogni autorizzato ha il dovere di prenderne visione e conoscerne il contenuto, oltre che di controllare periodicamente la documentazione in materia di privacy e sicurezza ivi pubblicata.

In caso di modalità di lavoro "Smart Working" la persona autorizzata, oltre alle presenti istruzioni impartite, deve seguire quelle comunicate a tutti i lavoratori.

Si precisa che gli obblighi sopra descritti rientrano nell'ambito della prestazione lavorativa e la violazione delle presenti istruzioni può comportare sanzioni disciplinari.

La presente autorizzazione ha efficacia fino alla risoluzione del rapporto di lavoro per qualsiasi causa oppure fino a revoca.

Gli obblighi relativi alla riservatezza, alla comunicazione ed alla diffusione dovranno essere osservati anche in seguito a modifica dell'incarico e/o cessazione del rapporto di lavoro.