ISTRUZIONI OPERATIVE PER GLI INCARICATI AL TRATTAMENTO DEI DATI PERSONALI

Gli incaricati, in relazione alle attività correlate all'incarico attribuito, devono porre in essere tutte le azioni necessarie a garantire che i trattamenti di dati personali effettuati avvengano nel rispetto delle disposizioni normative vigenti in materia di trattamento dei dati, compreso il profilo relativo alla sicurezza, e delle disposizioni aziendali.

PRINCIPI GENERALI

Gli incaricati devono:

- ✓ Trattare i dati di propria competenza nel rispetto dei principi di liceità, correttezza e trasparenza. In attuazione del: principio di minimizzazione dei dati: trattare i soli ed esclusivi dati personali che si rilevino necessari rispetto alle finalità per le quali sono trattati nell'attività a cui ciascun autorizzato è preposto; principio di limitazione delle finalità: trattare i dati conformemente alle finalità istituzionali del Titolare, limitando il trattamento esclusivamente a dette finalità; principio di esattezza: garantire l'esattezza, la disponibilità, l'integrità nonché il tempestivo aggiornamento dei dati personali oggetto di trattamento e verificare la pertinenza, completezza e non eccedenza rispetto alle finalità per le quali sono stati raccolti, e successivamente trattati.
- ✓ Utilizzare le informazioni e i dati personali, in particolare i dati c.d. dati particolari, con la massima riservatezza, sia nei confronti dell'esterno che del personale interno, per tutta la durata dell'incarico ed anche successivamente al termine di esso.
- ✓ Conservare i dati rispettando le misure di sicurezza, predisposte dal Titolare e/o dal Referente privacy di afferenza, garantendone la massima protezione in ogni attività di trattamento.
- ✓ Segnalare al Referente privacy di afferenza eventuali circostanze che rendano necessario od opportuno l'aggiornamento delle predette misure di sicurezza al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.
- ✓ Astenersi dal comunicare a terzi e/o dal diffondere dati ed informazioni appresi in occasione dell'espletamento della propria attività.
- ✓ Partecipare ai corsi formativi in materia di protezione dei dati personali e di sicurezza informatica con le modalità che verranno indicate dal Titolare del trattamento o da suo delegato.
- ✓ Collaborare alla implementazione e aggiornamento del Registro delle attività di trattamento del Titolare, con le modalità definite dal Comitato Data Protection e secondo le istruzioni ricevute, anche mediante utilizzo di apposito applicativo;
- ✓ coinvolgere tempestivamente e adeguatamente, in tutte le questioni riguardanti la protezione dei dati personali, il Responsabile della protezione dei dati (DPO) e collaborare con il medesimo per ogni questione relativa al trattamento dei dati personali, consentendo lo svolgimento di verifiche e audit presso la propria struttura;
- ✓ raccordarsi tempestivamente con il Titolare e con il DPO nei casi di violazione di sicurezza che comporta violazione dei dati;
- ✓ assicurare che la comunicazione a terzi delle categorie particolari di dati personali, e dei dati relativi alle condanne penali e reati avvengano solo se previste da norma di legge o di regolamento;

OPERAZIONI SPECIFICHE

Trattamento dati degli interessati

- ✓ Identificazione degli interessati: nell'ambito dell'accesso alle prestazioni, l'incaricato al trattamento può avere necessità di dover identificare il richiedente un servizio o il soggetto che deve presentare una istanza o una dichiarazione. Si deve procedere a tale verifica con rispetto della volontà dell'interessato, che deve essere invitato con cortesia ad esibire un proprio documento di identità, secondo quanto previsto dall'art.45 del DPR 445/2000 e nel rispetto di eventuali indicazioni operative aziendali;
- ✓ Raccolta dei dati: prima di procedere all'acquisizione dei dati personali devono essere fornite le informazioni all'interessato o alla persona presso cui si raccolgono i dati, secondo quanto stabilito dagli artt.13 e 14 del Regolamento (UE) 2016/679. Occorre procedere alla raccolta dei dati con la massima cura, verificando l'esattezza dei dati stessi;
- ✓ Gestione dei dati e dei documenti: non lasciare a disposizione di estranei supporti, fogli, cartelle e quant'altro;
- ✓ consegna di copie dei documenti: è necessario richiedere apposita delega e fare attenzione che l'invio di comunicazioni o di documentazione sanitaria al domicilio del paziente deve essere sempre preceduto dall'autorizzazione di questi ed essere sempre contenuto in busta sigillata, evitando di riportare sulla busta esterna riferimenti a servizi/strutture specifici dell'Azienda che possano in qualche modo essere idonei a rivelare lo stato di salute dell'interessato o a creare una forma di associazione con una qualsivoglia patologia.
- ✓ verificare periodicamente che il trattamento e le sue modalità di esecuzione siano coerenti con le funzioni istituzionali dell'Azienda, con le attività di competenza della struttura o incarico assegnato e con la specifica attività in connessione della quale il trattamento viene effettuato;
- ✓ verificare periodicamente l'esattezza e l'aggiornamento dei dati, nonché la loro pertinenza, completezza, non eccedenza e necessità rispetto alle finalità determinate per cui sono stati raccolti e per le ulteriori finalità con esse compatibili; verificare periodicamente che le modalità del trattamento garantiscano comunque il diritto alla riservatezza dei soggetti terzi;
- ✓ garantire la preventiva acquisizione del consenso nei casi in cui la normativa lo preveda;
- ✓ garantire la corretta custodia e la riservatezza dei documenti cartacei utilizzati per le attività di competenza, non lasciando incustodita o esposta alla visione di soggetti comunque non legittimati (compresi altri incaricati non abilitati al trattamento) la documentazione cartacea, ed in particolare controllare e custodire fino alla restituzione gli atti e i documenti contenenti le categorie di dati di cui agli artt. 9 e 10 del GDPR;
- ✓ in particolare, riporre i documenti che contengono le categorie di dati di cui agli artt. 9 e 10 del GDPR in archivi ad accesso controllato (armadi/schedari/contenitori muniti di serratura oppure soggetti a sorveglianza da parte di personale a ciò deputato);

Utilizzo strumenti aziendali

- ✓ Per le banche dati informatiche, utilizzare sempre il proprio codice di accesso personale, evitando di operare su terminali a disposizione altrui e/o di lasciare avviato, in caso di allontanamento anche temporaneo dalla postazione di lavoro, il sistema operativo con inserita la propria password, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento;

- ✓ Mail e uso della internet: la posta elettronica può essere utilizzata per scopi di ufficio. Occorre prestare particolare attenzione alla spedizione, a mezzo di posta elettronica, di files o di messaggi contenenti dati riferiti alla salute.
- ✓ Uso di software: è vietato installare e usare qualunque software senza la previa autorizzazione del Titolare e/o Suo delegato. Si ricorda che l'uso di software contraffatto, ovvero senza licenza d'uso, costituisce un illecito di natura sia penale sia civile, secondo quanto previsto dalla legge sul diritto d'autore (legge 633/1941), così come integrata dal d.lgs.518/1992 e ss.mm. ed ii.
- ✓ Protezione degli strumenti di lavoro: in caso di assenza, anche momentanea, dalla propria postazione di lavoro, devono essere adottate misure idonee ad escludere che soggetti non autorizzati possano acquisire la conoscenza di informazioni o accedere alle banche dati. A tal proposito, a titolo meramente esemplificativo, si consiglia di adottare un sistema di oscuramento (c.d. screensaver) dotato di password, ovvero di uscire dal programma che si sta utilizzando o, in alternativa, occorrerà porre lo strumento elettronico in dotazione in posizione di stand-by o spegnere l'elaboratore che si sta utilizzando. In caso di abbandono, anche temporaneo, dell'ufficio, l'autorizzato deve porre la massima attenzione a non lasciare incustoditi i documenti cartacei contenenti dati riferiti alla salute e altri tipologie di dati c.d "particolari" (es. adesione ad un sindacato) sulla scrivania o su tavolini di reparto: è infatti necessario identificare un luogo sicuro di custodia che dia adeguate garanzie di protezione da accessi non autorizzati (es. un armadio o un cassetto chiusi a chiave, una cassaforte, etc.);
- ✓ evitare, in particolare, di lasciare la propria stazione di lavoro incustodita e collegata con il proprio account all'ambiente di rete, chiudendola o bloccandola in tutte le occasioni in cui si assenti dall'ufficio;
- ✓ utilizzare, per l'accesso alle banche dati automatizzate, il proprio codice personale, al fine di consentire sempre l'individuazione di chi ha effettuato una operazione di trattamento;
- ✓ non utilizzare la rete aziendale per fini non espressamente autorizzati e tiene un comportamento corretto durante la navigazione in internet;
- ✓ evitare di alterare la configurazione software della stazione di lavoro.
- ✓ controllare che ogni dispositivo idoneo a stampare documenti sia disposto in modo che la visione dei documenti in uscita sia possibile solo da parte del personale incaricato al trattamento dei dati, attivando in caso contrario il Preposto al trattamento e, in caso di utilizzo di stampanti, fotocopiatrici o fax condivisi da vari utenti e collocati al di fuori dei locali ove è posta la singola stazione di lavoro, raccogliere immediatamente le stampe e le custodisce con le modalità sopra descritte;

Per il Regolamento aziendale per l'utilizzo delle risorse informatiche dell'Azienda Meyer si rinvia all'apposito allegato approvato dalla Direzione Generale.

Attività riguardanti rapporto con gli interessati

- ✓ Rispetto della distanza di sicurezza: per quanto riguarda gli operatori di sportello deve essere prestata attenzione al rispetto dello spazio di cortesia e se del caso devono essere invitati gli utenti a sostare dietro la linea tracciata sul pavimento ovvero dietro le barriere delimitanti lo spazio di riservatezza;
- ✓ Obbligo di riservatezza e segretezza: mantenere l'assoluta segretezza sulle informazioni di cui si venga a conoscenza nel corso delle operazioni di trattamento. La diffusione di dati idonei a rivelare lo stato di salute è tassativamente vietata;
- ✓ Controllo dell'identità del richiedente nel caso di richieste di comunicazioni di dati (presentate per telefono): occorre verificare l'identità del soggetto richiedente, ad esempio formulando una serie di quesiti (accertamento sommario).

- ✓ assicurare che gli ordini di precedenza e di chiamata per prestazioni sanitarie prescindano dalla individuazione nominativa degli interessati;
- ✓ in caso di richiesta o di fruizione di prestazioni sanitarie e/o amministrative, porre in essere tutte le misure individuate dal Preposto al trattamento finalizzate delimitare apposite distanze di cortesia o comunque atte a garantire la riservatezza degli utenti;
- ✓ non esporre al pubblico, nei reparti o in altri locali, i nominativi dei pazienti ricoverati, né liste nominative di prestazioni ambulatoriali, di diagnostica strumentale e di laboratorio e di altre prestazioni sanitarie in genere;
- ✓ dare informazioni, anche per telefono, limitatamente alla presenza di una persona al pronto soccorso o in reparto (senza dare notizie sullo stato di salute) solo a terzi legittimati (parenti, familiari, conviventi, conoscenti, volontari), in ogni caso rispettando l'eventuale volontà contraria espressa dal paziente e raccolta al momento dell'accesso;
- ✓ non utilizzare strumenti di social networking per la condivisione di dati personali riferiti a pazienti;
- ✓ non raccogliere immagini dei pazienti mediante dispositivi elettronici di ripresa non autorizzati, inclusi telefoni cellulari.

RESPONSABILITA'

Gli incaricati rispondono al Titolare per l'inosservanza delle presenti istruzioni nonché per la violazione o inadempimento di quanto previsto dalla normativa in materia di protezione dei dati personali (fatte salve ulteriori fattispecie di responsabilità penale, a titolo personale, nonché amministrativa e contabile in sede di rivalsa).

Il ruolo di soggetto autorizzato al trattamento dei dati non è suscettibile di delega. In caso di assenza o impedimento, le relative attribuzioni competono a chi lo sostituisce nell'attività istituzionale. La preposizione al trattamento è connessa all' incarico conferito, per cui viene automaticamente meno alla scadenza o alla revoca dell'incarico cui è correlata.

Gli obblighi sopra descritti fanno parte integrante della prestazione lavorativa e pertanto, per il personale dipendente o assimilato, sono dovuti in base al contratto di lavoro sottoscritto con l'Azienda Meyer.

Le istruzioni di cui sopra sono altresì integrate dalle puntuali disposizioni aziendali in materia di protezione dei dati personali a cui si rinvia, reperibili alla pagina intranet dedicata.