Istruzioni per i responsabili, i designati e gli incaricati in materia di trattamento dei dati personali

(art. 29 e 32 del Regolamento (UE) 2016/679, art. 2-quaterdecies del D. Lgs. n. 196/2003)

Indice

Premessa

Scopo del presente documento è illustrare le norme comportamentali, organizzative e tecniche cui i responsabili esterni, i soggetti designati e gli incaricati devono attenersi nello svolgimento delle operazioni di trattamento dei dati personali, al fine di ridurre e contenere i rischi di danneggiamento o dispersione, perdita dei dati trattati dall'Azienda, a causa di un uso non corretto o illecito dei sistemi informatici e degli archivi cartacei.

1. Istruzioni generali

1.1. - Segreto professionale o d'ufficio

Tutti i soggetti designati e gli incaricati del trattamento dei dati **devono mantenere il segreto** sulle informazioni di cui vengono a conoscenza nello svolgimento della propria attività lavorativa e professionale e nel corso delle operazioni di trattamento, evitando di comunicare le informazioni a terzi.
Tutto il personale del ruolo sanitario, tecnico, professionale e amministrativo, sia del comparto che della dirigenza, e chiunque presti la propria attività lavorativa anche in veste di consulente, libero/professionista o tirocinante o volontario, nei servizi o strutture dell'Azienda è tenuto **al segreto professionale o al segreto d'ufficio**, ossia a non rivelare e/o agevolare in qualsiasi modo, senza giusta causa, la conoscenza di notizie, dati o banche dati di cui, in ragione e in occasione del proprio stato o ufficio, sia venuto a conoscenza. L'eventuale violazione di tale obbligo può comportare l'applicazione di sanzioni di natura deontologica e disciplinare, nonché una responsabilità di natura amministrativa, civile e penale, secondo quanto previsto dalla legge.

1.2. - Tutela della dignità della persona

Va sempre tutelata la dignità di tutti i soggetti che usufruiscono di prestazioni sanitarie, con particolare riguardo alle fasce deboli (ad es. disabili fisici o psichici, minori e anziani), pazienti sieropositivi o affetti da infezione da HIV, pazienti sottoposti a trattamenti medici invasivi, soggetti particolarmente vulnerabili (ad es. interruzione volontaria di gravidanza o vittime di atti di violenza sessuale o di genere).
Nelle terapie intensive o nei reparti che consentono la visione dei pazienti attraverso videoterminali, devono essere utilizzati paraventi o altri accorgimenti che limitino la visibilità dell'interessato, durante l'orario di visita, ai soli familiari e conoscenti.

1.3. - Riservatezza nei colloqui e nel corso di prestazioni sanitarie

Durante i colloqui con l'interessato, o con soggetti dallo stesso individuati, o durante l'esecuzione di prestazioni sanitarie vanno adottate cautele per evitare che le informazioni sulla salute possano essere conosciute da terzi. Analoghe cautele vanno adottate in occasione della raccolta di dati anamnestici, qualora avvenga in situazioni di promiscuità.
Tutti gli operatori devono evitare di discutere sulle condizioni cliniche dei pazienti in pubblico, nei luoghi comuni (corridoi, bar, ascensore), in presenza di estranei o con qualsiasi altra modalità (es. social network, videoconferenza, ecc.), con riferimenti che rendano direttamente o indirettamente identificabile la persona.

1.4. - Presenza in reparto o in Pronto Soccorso

Utilizzando la modulistica predisposta, l'interessato – se cosciente e capace – all'atto del ricovero o dell'accesso in PS deve essere informato e posto in condizione di fornire indicazioni circa i soggetti che possono ricevere notizie sul suo stato di salute e/o sulla sua presenza in reparto o PS.
Deve essere rispettata l'eventuale decisione dell'interessato di non rendere nota la sua presenza in ospedale.

1.5. - Comunicazione all'interessato o a terzi legittimati

La comunicazione al paziente di informazioni sul suo stato di salute deve essere effettuata solo da un medico o da altro operatore sanitario che intrattenga rapporti diretti con il paziente (ad esempio personale infermieristico autorizzato dal responsabile della UO/Servizio).
Le informazioni sullo stato di salute possono essere fornite a soggetti diversi dall'interessato solo se espressamente individuati dal medesimo, mediante la modulistica in uso, oppure nei casi previsti dalla legge.
Pertanto, prima di dare informazioni a terzi legittimati (ad esempio: coniuge, convivente, figli, genitori, fratelli, nonni, nipoti, ecc.) occorre verificare che il paziente non abbia espresso volontà contraria o abbia identificato solo particolari soggetti destinatari dell'informazione, accertandosi, per quanto ragionevole, dell'identità dei soggetti richiedenti.
Nel caso di pazienti minori con genitori separati con affidamento esclusivo, la comunicazione di notizie al genitore non affidatario può avvenire solo previo consenso esplicito di quello affidatario.
Con specifico riferimento ai dati particolari, le notizie da fornire, specie se destinate a soggetti terzi (es. medico di famiglia), devono limitarsi ai soli elementi pertinenti e necessari per le finalità di cura.

1.6. - Richiesta di notizie per telefono o ad organi di stampa

E' vietato fornire dati e informazioni di carattere sanitario per telefono ad eccezione dei pazienti e delle persone da questi autorizzate e solo se si abbia certezza assoluta dell'identità del chiamante.
Nel caso in cui giungano richieste telefoniche di dati sanitari da parte dell'Autorità Giudiziaria o degli organi di polizia occorre verificare preliminarmente l'identità del soggetto richiedente richiamando l'interlocutore al numero da questi comunicato.
È fatto divieto di comunicare dati personali o sanitari agli organi di stampa; le eventuali richieste di informazioni devono essere inoltrate alla Direzione Generale per il tramite dell'URP.

1.7. - Distanze di cortesia

Tutti i punti di accettazione e front office devono rispettare una distanza di cortesia, evidenziata da una striscia gialla di segnalazione posta a terra e da un avviso o cartello per l'utenza, sia per operazioni amministrative allo sportello (prenotazione, accettazione, ritiro referti), sia per l'acquisizione di dati personali comuni e relativi alla salute.

1.8. - Ordine di chiamata

Gli utenti in attesa di visita o di accertamenti (ad es. analisi cliniche o indagini di radiologia) non vanno chiamati per nome ma mediante chiamata non nominativa (eliminacode o attribuzione di un codice numerico o alfanumerico al momento dell'accettazione).

1.9. - Liste di pazienti

E' vietata l'affissione di liste di pazienti nei locali destinati all'attesa o comunque aperti al pubblico, con o senza la descrizione del tipo di patologia sofferta.

1.10. - Cartella clinica e documentazione sanitaria cartacea

In caso di trasferimento interno dei pazienti ricoverati tra i diversi Presidi o reparti o nel caso di consulenza o accertamenti diagnostici, la documentazione sanitaria va posta in buste o raccoglitori chiusi e non trasparenti, in modo da non permettere la lettura dei dati sensibili da parte di personale non autorizzato.
La documentazione va presa in custodia dal personale incaricato (infermiere o ausiliario) e da questi consegnata al reparto di trasferimento, o restituita al reparto di provenienza al termine della prestazione o consulenza.
I documenti e i supporti elettronici portati in visione dal paziente devono essere conservati rispettando le regole di tutela del segreto professionale e, al momento della dimissione o alla conclusione della visita, riconsegnati al paziente.

1.11. - Ritiro di referti

Qualsiasi documento relativo ad attività sanitarie (referti di esami di laboratorio o di esami strumentali, referti di Pronto Soccorso e di visite ambulatoriali, lettere di dimissione) deve essere consegnato in busta chiusa direttamente all'Interessato.
Il ritiro della documentazione sanitaria è ammesso anche da parte di persona diversa dall'interessato purché munita di delega scritta e con consegna in busta chiusa.
Per gli accertamenti HIV non è consentito il ritiro mediante delega.

1.12. - Invio di referti medici mediante posta elettronica

L'invio online di referti medici è facoltativo ed è consentito su richiesta dell'utente e previa informativa ed acquisizione di consenso esplicito a mezzo della modulistica dedicata. L'invio online non è consentito in caso di analisi genetiche o accertamenti HIV. I referti vanno allegati al messaggio previo utilizzo di sistemi di cifratura e con invio separato della password di apertura del file (rif. nota prot. 2301 del 11/03/2019).

1.13. - Attestazione di presenza in ospedale

Le dichiarazioni attestanti la visita, l'esame o il ricovero effettuati (es. giustificativo per il datore di lavoro) devono essere formulate in maniera tale che dalle stesse non possano derivare, per gli estranei, informazioni riguardanti lo stato di salute della persona interessata. L'attestazione deve essere generica e non deve riportare indicazioni sulla U.O. di erogazione, né il timbro con la specializzazione del sanitario o ogni altra informazione da cui si possa evincere la patologia sofferta (rif. nota prot. 5730 del 19/06/2019).

2. - Documentazione cartacea e sanitaria

2.1. - Tenuta e custodia

- I documenti contenenti dati personali o dati relativi alla salute, devono essere custoditi dagli incaricati del trattamento in modo da non essere accessibili a persone prive di autorizzazione fino al termine delle operazioni affidate (es. locali non accessibili al pubblico, armadi o cassetti chiusi a chiave).
- I documenti contenenti dati personali o dati particolari non devono rimanere incustoditi su scrivanie o tavoli di lavoro.
- In caso di locali aperti al pubblico, le cartelle e i fascicoli del lavoro devono essere tenuti sulla propria scrivania facendo sì che i dati non siano visibili a persone non autorizzate.
- In caso di assenza o allontanamento, anche temporaneo, dalla postazione di lavoro, è vietato lasciare incustoditi fascicoli, cartelle o documenti cartacei contenenti dati particolari. In tal caso occorre chiudere la propria stanza, qualora rimanga incustodita senza personale all'interno, oppure riporre la documentazione in un armadio o cassetto chiuso a chiave.

2.2. - Comunicazione e trasmissione

- I documenti contenenti dati personali non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative (anche se queste persone sono a loro volta incaricate del trattamento).
- I documenti vanno consegnati ai destinatari utilizzando buste chiuse o raccoglitori sigillati a garanzia dell'integrità, oppure effettuando la consegna personalmente, in modo da ridurre al minimo la possibilità che soggetti terzi non autorizzati possano prendere visione del contenuto.
- L'invio di documentazione sanitaria al domicilio del paziente, su richiesta dello stesso, deve avvenire in busta chiusa ed evitando di riportare sulla busta esterna riferimenti a specifici servizi/strutture dell'Azienda che possano rivelare lo stato di salute dell'interessato o il tipo di patologia.
- Nel trasporto della documentazione tra un ufficio e l'altro, occorre adottare precauzioni per evitare la visibilità dei dati personali da parte di estranei (ad es. carpette o faldoni anonimi).
- In caso di dati riservati o relativi alla salute occorre accertarsi che il tipo di spedizione sia idoneo a garantire l'integrità della documentazione e la ricezione certa da parte del destinatario.
- E' proibito trasportare all'esterno del posto di lavoro qualsiasi documentazione contenente dati personali e particolari, salvo motivate esigenze di servizio e fermi restando gli obblighi di custodia.

2.3. - Archiviazione e distruzione

- I documenti cartacei contenenti dati sensibili e/o giudiziari devono essere utilizzati dagli incaricati solo per il tempo necessario allo svolgimento dei relativi compiti e poi riposti in archivi o locali ad accesso controllato o, nei casi previsti, affidati al servizio di archiviazione.
- Qualora sia necessario disfarsi di documenti cartacei contenenti dati personali, questi devono essere distrutti utilizzando gli appositi distruggidocumenti o, in loro assenza, strappandoli manualmente in modo da non essere più ricomponibili o leggibili.

3. – Uso di strumenti informatici

3.1. – User-id e password

- L'accesso alle risorse informatiche dell'Azienda (PC, applicativi, banche dati, posta elettronica, ecc) è consentito agli incaricati dotati di credenziali di autenticazione formate da un codice di accesso (user-id o username) e da una parola chiave riservata (password) conosciuta solamente dal medesimo.
- Il CED, o l'amministratore di sistema, assegna a ciascun incaricato una user-id, riconducibile ad una singola persona, ed una password temporanea da modificare alla prima connessione.
- La password scelta dall'utente deve essere sufficientemente "robusta": minimo 8 caratteri alfanumerici, caratteri speciali, lettere maiuscole e minuscole.
- La password va cambiata periodicamente ogni sei mesi o secondo le specifiche scadenze comunicate dal CED. Va inoltre cambiata in ogni caso di sospetto utilizzo o conoscenza da parte di terzi.
- La password deve essere conservata con la massima attenzione e segretezza e non deve essere comunicata a terzi o lasciata in luoghi accessibili a terzi.
- User-id e password non devono mai essere condivise tra più utenti (anche se incaricati del trattamento).
- Solo per motivate esigenze di servizio (ad es. in caso di assenza dal servizio) le credenziali possono essere rese note al responsabile dell'UO.

3.2. - Posta elettronica

- Ogni utente deve utilizzare la posta elettronica messa a disposizione dall'Azienda esclusivamente per necessità di lavoro e lo scambio di corrispondenza tra l'interessato e i propri familiari, amici e conoscenti deve essere assolutamente limitato nel tempo e nella quantità.
- La casella di posta è assegnata in maniera nominale ed univoca ad una persona fisica, pertanto ogni utente è direttamente responsabile sia da un punto di vista disciplinare che giuridico del suo utilizzo e del contenuto dei messaggi inviati.
- Nell'invio di una email occorre prestare massima attenzione alla corretta digitazione dell'indirizzo del destinatario, specie in caso di comunicazioni riservate o relative alla salute.
- L'indirizzo mail aziendale non deve essere utilizzato per l'iscrizione a servizi (social network, gruppi di discussione, servizi telefonici, bancari, assicurativi di tipo personale etc.) non strettamente correlati alla propria attività istituzionale.
- L'utente non deve aprire o rispondere a mail inattese e/o di provenienza incerta o sospetta, anche se sembrano provenire da un mittente affidabile, mail contrassegnate come indesiderate (spam), mail contenenti allegati o link di cui non si conosce la natura e l'origine (estensione .com .exe .vbs .scr .pif ecc), che possono contenere file o programmi dannosi capaci di diffondere virus o programmi malevoli nell'infrastruttura aziendale o costituire attività di "phishing" mirate al furto di dati personali.
- E' vietato, tranne che per motivate esigenze di servizio, l'accesso alla mail aziendale da computer pubblici in quanto alcuni dati potrebbero essere temporaneamente memorizzati nel disco locale e recuperati da un altro utente, se non cancellati in modo corretto.
- E' altresì vietato l'accesso alla mail aziendale mediante wifi-pubblici (ad es. aeroporti, hotel, ristoranti, ecc.) o altre reti non protette che espongono a rischi per la sicurezza dei dati.

3.3. - Personal computer

- Il PC in dotazione va utilizzato esclusivamente per ragioni di lavoro e per conto dell'Azienda.
- In caso di necessità, i dipendenti possono utilizzare un PC aziendale diverso da quello in dotazione, entrando in rete con la propria username e password.
- Durante la sessione di lavoro è necessario evitare che persone estranee e non autorizzate possano visualizzare la schermata del PC posizionando, se del caso, lo schermo in modo da limitarne la visibilità.
- Durante una sessione di lavoro non lasciare il PC incustodito o accessibile da soggetti estranei: in caso di allontanamento, anche temporaneo, dalla postazione di lavoro disconnettere la sessione di lavoro premendo la combinazione Ctrl+Alt+Canc oppure impostare uno screensaver con password.
- Chiudere i programmi secondo le appropriate misure di sicurezza per evitare la perdita dei dati.
- Spegnere il PC al termine della sessione lavorativa o in caso di assenza prolungata dalla postazione di lavoro.
- Non apportare modifiche alle impostazioni di sicurezza o di configurazione del PC (es. antivirus) né installare software o hardware diversi da quelli forniti dall'Azienda senza formale autorizzazione del CED. L'uso di software contraffatto, ovvero senza licenza d'uso, costituisce un illecito penale e civile, secondo quanto previsto dalla legge sul diritto d'autore.
- Provvedere al regolare aggiornamento del PC e non interrompere le operazioni di aggiornamento pianificate procedendo al salvataggio dei dati ed al riavvio del PC, qualora richiesto.
- I dati e i documenti elettronici contenenti dati particolari vanno archiviati sul server centrale dell'Azienda ed eliminati dall'hard disk del PC in dotazione.
- E' vietata la condivisione di documenti contenenti dati personali particolari su cloud e server non aziendali.

3.4. - Dispositivi portatili e supporti di memoria

- I dispositivi portatili (notebook, tablet, ecc) e i supporti di memoria rimovibili (ad es. CD, DVD, pen drive, memorie USB, ecc) devono essere conservati in un luogo sicuro (stanze, armadi o cassetti chiusi a chiave) e non vanno lasciati incustoditi.
- E' vietato l'uso di dispositivi portatili e memorie al di fuori dall'Azienda, tranne che per motivate esigenze di servizio. L'utilizzatore è personalmente consapevole dei rischi per la protezione dei dati e delle conseguenti responsabilità in caso di perdita o violazione degli stessi.
- Salvo motivate esigenze, è tassativamente vietato trasferire, anche solo temporaneamente, copie di dati personali particolari (es. dati sanitari) su qualsiasi dispositivo portatile o memoria rimovibile.
- Nel caso in cui vi sia la motivata necessità di memorizzare dati relativi alla salute su dispositivi portatili o memorie rimovibili, l'archiviazione deve avvenire mediante impiego di idonei sistemi di crittografia e copie di backup.
- Al momento di rimuovere i dispositivi di memoria seguire le procedure di disconnessione sicura.
- Assicurarsi che i dispositivi non vengano utilizzati da terzi e che non siano infettati da virus (procedere alla scansione del supporto).
- E' vietata, tranne che per motivate esigenze di servizio, la connessione dei dispositivi aziendali a wifi-pubblici (ad es. aeroporti, hotel, ristoranti, ecc.) o altre reti non protette, in quanto comportano rischi per la sicurezza dei dati.
- In caso di riutilizzo/dismissione dei dispositivi portatili e dei supporti di memoria, l'utente deve assicurarsi che si proceda, prima dello smaltimento, all'eliminazione permanente delle informazioni e dei dati memorizzati affinché questi non possano essere in alcun modo recuperati.

3.5. - Fotocopiatrici, stampanti e fax

- Assicurarsi di non lasciare incustodite le stampe contenenti dati sensibili, specie se la stampante o la fotocopiatrice è condivisa con più utenti e si trova a distanza dalla postazione informatica. Le copie non necessarie devono essere rese illeggibili prima di essere eliminate.
- L'apparecchio fax deve essere sempre collocato in un luogo non accessibile a terzi non autorizzati.
- In caso di ricevimento via fax di documentazione contenente dati personali particolari provvedere all'immediato ritiro della stessa.
- Non lasciare incustoditi presso il fax documentazione contenente dati personali e particolari.
- Prima di inviare via fax documenti contenenti dati relativi alla salute assicurarsi preventivamente che l'effettivo destinatario sia sul posto o comunque che il fax sia in un luogo protetto e presidiato, non accessibile a pubblico, e che non vi siano pertanto rischi di conoscenza da parte di soggetti estranei o non autorizzati.
- In fase di invio del fax prestare la massima attenzione alla corretta digitazione del numero del destinatario.
- Sulla copertina del fax si consiglia di apporre la seguente formula: "Qualora il destinatario del presente fax non sia la persona indicata nella presente copertina, è pregato di dare immediata comunicazione al mittente, a mezzo telefono o per fax. Il destinatario della presente comunicazione deve distruggere immediatamente la documentazione ricevuta e in ogni caso potrà essere ritenuto responsabile dell'uso non autorizzato delle informazioni ivi contenute, erroneamente acquisite".