Istruzioni specifiche per l'ambito sanitario destinate sia ai Responsabili del trattamento sia agli Autorizzati al trattamento della LDB Medical Care

Indice

Premessa

1. - Istruzioni generali
1.1 - Segreto professionale o d'ufficio
1.2 - Tutela della dignità della persona
1.3 - Riservatezza nei colloqui e nel corso di prestazioni sanitarie
1.4 - Comunicazioni sulla presenza del Paziente nelle strutture della LDB Medical Care
1.5 - Comunicazione all'interessato o a terzi legittimati
1.6 - Rilascio notizie a mezzo telefono o ad organi di stampa
1.7 - Distanze di cortesia
1.8 - Ordine di chiamata
1.9 - Liste dei pazienti
1.10 - Documentazione sanitaria
1.11 - Ritiro referti

2. Documentazione cartacea e sanitaria
2.1. - Tenuta e custodia
2.2. - Comunicazione e trasmissione
2.3. - Archiviazione e distruzione

3. Uso di strumenti informatici
3.1. - User-id e password
3.2. - Posta elettronica
3.3. - Personal computer
3.4. - Dispositivi portatili e supporti di memoria
3.5 - Sistemi server e Backup
3.6. - Fotocopiatrici, stampanti e fax

PREMESSA

Le presenti istruzioni – integrative delle precedenti n. 7 e con specifico riferimento all'ambito sanitario - hanno lo scopo di chiarire e diffondere regole/misure comportamentali, organizzative e tecniche cui i designati Responsabili del trattamento e gli Autorizzati al trattamento devono attenersi nello svolgimento delle operazioni di trattamento dei dati personali all'interno dell'organizzazione della LDB Medical Care al fine di ridurre e contenere i rischi di danneggiamento, dispersione o perdita di dati 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 designati in qualità di Responsabili del trattamento e gli Autorizzati al trattamento sono tenuti a mantenere la necessaria riservatezza 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 informazioni e dati a terzi.

Tutto il personale della LDB Medical Care e la dirigenza – appartenente al ruolo sanitario, tecnico, professionale e amministrativo - e chiunque presti la propria attività lavorativa (anche in veste di consulente, libero/professionista, tirocinante, volontario, specializzando) presso le strutture della LDB Medical Care 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

Deve essere 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).

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 opportune 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 i professionisti e operatori devono evitare di discutere sulle condizioni cliniche dei pazienti in pubblico, nei luoghi comuni (es. corridoi, bar, ascensore), in presenza di estranei o mediante o utilizzando altre modalità, quali social network, videoconferenza pubblica, ricorrendo a riferimenti che rendano direttamente o indirettamente identificabile la persona.

1.4 - Comunicazioni sulla presenza del Paziente nelle strutture della LDB Medical Care

Utilizzando la modulistica appositamente predisposta, l'interessato – se cosciente e capace – all'atto dell'accesso alle strutture della LDB Medical Care 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 presso le diverse strutture della LDB Medical Care. Deve essere rispettata l'eventuale decisione dell'interessato di non rendere nota la sua presenza.

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 personale medico o da altro operatore sanitario che intrattenga rapporti diretti con il paziente (ad esempio personale infermieristico autorizzato).

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, ecc.) occorre verificare che il paziente non abbia espresso volontà contraria o abbia identificato solo particolari soggetti destinatari dell'informazione, accertandosi - per quanto possibile - 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 alle categorie particolari di dati personali, 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 - Rilascio notizie a mezzo telefono o ad organi di stampa

E' vietato fornire dati e informazioni di carattere sanitario tramite 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 al DPO.

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 o visite) non devono essere chiamati direttamente per nome o cognome ma mediante chiamata non nominativa (elimina-code, numero di prenotazione 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 - Documentazione sanitaria

Nel caso di consulenza o accertamenti diagnostici la documentazione sanitaria del paziente deve essere riposta in buste o raccoglitori chiusi e non trasparenti, in modo da non permettere la lettura dei dati sensibili da parte di personale non autorizzato. I documenti e i supporti elettronici portati in visione dal paziente devono essere conservati rispettando le regole del rispetto del segreto professionale e, al momento della conclusione della visita, riconsegnati al paziente.

1.11. - Ritiro referti

Qualsiasi documento relativo ad attività sanitarie, portati in visione dagli utenti/pazienti (quali referti di esami di laboratorio o di esami strumentali, referti di Pronto Soccorso e di visite ambulatoriali, lettere di dimissione) deve essere riconsegnato in busta chiusa nelle proprie mani dell'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.

2 - DOCUMENTAZIONE CARTACEA E SANITARIA

2.1 - Tenuta e custodia

I documenti contenenti dati personali o dati relativi alla salute del Paziente, devono essere custoditi dai designati in qualità di Autorizzati al trattamento in modo da non essere accessibili a persone prive di autorizzazione (es. locali non accessibili al pubblico, armadi o cassetti chiusi a chiave). I documenti contenenti dati personali o dati relativi alla salute del Paziente non devono rimanere incustoditi su scrivanie o tavoli di lavoro.

In caso di locali aperti al pubblico, le cartelle e i fascicoli 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 relativi alla salute del Paziente. 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 colleghi che non ne necessitano per lo svolgimento delle proprie mansioni lavorative (anche se tali professionisti o operatori sono a loro volta Autorizzati al trattamento).

I documenti contenenti dati personali devono essere 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.

La trasmissione 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 Direzioni/Uffici/Unità Operative della LDB Medical Care 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 comuni e appartenenti a categorie 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 dai designati in qualità di Autorizzati al trattamento solo per il tempo necessario allo svolgimento dei relativi compiti istituzionali 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 distruggi-documenti o, in loro assenza, strappandoli manualmente in modo da non essere più ricomponibili o leggibili.

3 - UTILIZZO DI STRUMENTI INFORMATICI

3.1 - User-id e password

- L'accesso alle risorse informatiche della LDB Medical Care (PC, applicativi, banche dati, posta elettronica, ecc.) è consentito agli Autorizzati al trattamento 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 **Responsabile IT** rilascia le credenziali utente in qualità di Amministratore di Sistema. Nella richiesta di rilascio credenziali devono essere riportati obbligatoriamente i recapiti di telefono della LDB Medical Care e di telefono personale, generalità, Codice Fiscale, Direzione/Ufficio/ Unità Operativa di appartenenza dell'utente assegnatario della nuova user-id, riconducibile ad una singola persona. Provvederà alla abilitazione creando una password temporanea da modificare alla prima connessione.
- La password scelta dall'utente deve essere complessa, composta da almeno 8 caratteri alfanumerici, caratteri speciali (,.!?-=;:), lettere maiuscole, lettere minuscole e numeri.
- La password deve essere cambiata periodicamente almeno ogni sei mesi o secondo le specifiche scadenze appositamente comunicate. 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 collocata a vista o in prossimità sulle postazioni di lavoro, non deve essere comunicata a terzi o lasciata in luoghi accessibili a terzi.
- User-id e password sono personali e non devono mai essere condivise tra più utenti anche se autorizzati al trattamento.
- Solo per motivate esigenze di servizio (ad es. in caso di assenza dal servizio) le credenziali possono essere rese note al responsabile della Direzione/Ufficio/Unità Operativa.

3.2 - Posta elettronica

- Ogni utente deve utilizzare la posta elettronica messa a disposizione dalla LDB Medical Care 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 elettronica 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 e-mail occorre prestare massima attenzione alla corretta digitazione dell'indirizzo del destinatario, specie in caso di comunicazioni riservate o relative alla salute.
- L'indirizzo di posta elettronica aziendale non deve essere utilizzato per l'iscrizione a servizi (social network, gruppi di discussione, servizi telefonici, bancari, assicurativi di tipo personale ecc.) non strettamente correlati alla propria attività istituzionale.
- L'utente non deve aprire o rispondere a comunicazioni e-mail inattese e/o di provenienza incerta o sospetta (anche se sembrano provenire da un mittente affidabile), contrassegnate come indesiderate (spam), 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 – ad eccezione di motivate esigenze di servizio - l'accesso alla casella di posta elettronica 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 casella di posta elettronica aziendale mediante wifi-pubblici (ad es. aeroporti, hotel, ristoranti, ecc.) o altre reti non protette che espongono a rischi per la sicurezza dei dati.
- Ogni utente deve periodicamente cancellare o archiviare la posta elettronica in modo da evitare il riempimento della quota disco assegnata.
- Ogni utente deve predisporre, nell'ambito dell'apposita area "Preferenze" > "Firme" della *webmail*, la firma in fondo ai messaggi avendo cura di dettagliare identità, Direzione/Ufficio/ Unità Operativa di appartenenza, numeri di telefono di contatti.

3.3 - Personal computer
- Il PC in dotazione deve essere utilizzato esclusivamente per ragioni di lavoro e per conto della LDB Medical Care.
- E' vietato connettere alla rete dati aziendale personal computer personali.
- 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 di dominio.
- 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 si deve lasciare il PC incustodito o accessibile da soggetti estranei: in caso di allontanamento - anche temporaneo - dalla postazione di lavoro occorre bloccare la postazione o disconnettere la sessione di lavoro.
- I programmi devono essere chiusi secondo appropriate misure di sicurezza per evitare la perdita dei dati.
- Il PC deve essere spento al termine della sessione lavorativa o in caso di assenza prolungata dalla postazione di lavoro, salvo diversa indicazione per necessità di accesso in *smartworking*.
- Gli unici addetti autorizzati ad installare software, apportare modifiche alle impostazioni di sicurezza o di configurazione del PC (es. antivirus) sono i tecnici del **Service**. Nessun utente è autorizzato ad installare software o hardware diversi da quelli forniti dalla LDB Medical Care senza formale autorizzazione del Titolare. L'uso di software contraffatto, ovvero con licenza d'uso contraffatta, costituisce un illecito penale e civile, secondo quanto previsto dalla normativa sul diritto d'autore.
- Ogni utente è tenuto a non interrompere le operazioni di aggiornamento pianificate del sistema operativo e degli antivirus, procedendo al salvataggio dei dati ed al riavvio del PC, qualora richiesto
- I dati e i documenti elettronici contenenti dati sensibili devono essere archiviati sul server cloud dedicato ed eliminati dall'hard disk del PC in dotazione.

3.4 - Dispositivi portatili e supporti di memoria
- I dispositivi portatili (notebook, tablet, ecc.) e i supporti di memoria rimovibili (ad es. CD, DVD, pendrive, 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 delle Direzioni/Uffici/Unità Operative della LDB Medical Care, 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.
- In sede di rimozione dei dispositivi di memoria occorre seguire le procedure di disconnessione sicura.
- E' obbligatorio assicurarsi che i dispositivi non vengano utilizzati da terzi e che non siano infettati da virus (procedere alla scansione del supporto).
- E' vietata, ad eccezione di 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.
- n 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 - Sistemi server e Backup
- E' obbligatorio utilizzare i software e le app cloud autorizzare dalla LDB Medical Care per detenere dati aziendali necessari alle continuità di servizio.
- E' consigliato verificare almeno settimanalmente la presenza e consistenza dei dati contenuti nelle cartelle e comunicare tempestivamente eventuali errate cancellazioni dei medesimi. Il sistema informatico possiede una data retention per i dati utenti di 7 giorni. In caso di cancellazione di file con tempo superiore sarà impossibile recuperare i backup dei medesimi.

3.6 - Fotocopiatrici, stampanti e fax
- Occorre 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.
- Fotocopiatrici, fax, stampanti di rete, devono essere sempre collocate in un luogo non accessibile a terzi non autorizzati.
- In caso di ricevimento via fax di documentazione contenente dati sensibili occorre provvedere all'immediato ritiro della stessa.
- Non si deve lasciare incustodita presso fotocopiatrici, fax, stampanti di rete documentazione contenente dati sensibili.
- Prima di inviare via fax documenti contenenti dati relativi alla salute occorre 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 occorre 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".

Roma, 1 febbraio 2022

Il Data Protection Officer