SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Ospedaliero - Universitaria di Ferrara

Università degli Studi di Ferrara

ISTRUZIONI AI SOGGETTI AUTORIZZATI AL TRATTAMENTO DEI DATI PERSONALI

Sommario

1. Premessa.

Il "soggetto autorizzato al trattamento" è colui che tratta i dati personali di titolarità dell'Azienda e che, quindi, all'atto dell'assunzione e/o della formalizzazione del rapporto di collaborazione, nonché, successivamente, in caso di trasferimento e/o di mutamento di mansioni, o comunque in ogni caso in cui l'Azienda ritenga opportuno procedervi, viene autorizzato al trattamento dei dati personali del Servizio al quale lo stesso è assegnato (ai fini della sua individuazione si invita il soggetto autorizzato a verificare nel proprio contratto e/o nella documentazione relativa al rapporto di lavoro la relativa assegnazione).

La relativa autorizzazione è disciplinata dagli art. 29 del Reg. UE 679/2016 (c.d. RGPD) e dall'art. 2-*quaterdecies* del D.Lgs. 30 giugno 2003 n. 196 e impone al soggetto autorizzato di rispettare le istruzioni sul trattamento dei dati comunque fornite dal "datore di lavoro", ovvero dall'intestata Azienda, così come gli impongono di seguire i corsi di formazione organizzati dall'Azienda stessa ed aventi ad oggetto, appunto, il trattamento e la protezione dei dati personali.

Il singolo soggetto autorizzato, pertanto, è autorizzato a svolgere operazioni di trattamento, per il proprio ambito di competenza, secondo i principi generali di trattamento, le prescrizioni, le istruzioni operative generali di seguito impartite dal Titolare e le ulteriori eventuali istruzioni specifiche impartite dall'Azienda in specifici contesti che non sono oggetto del presente documento.

Gli obblighi sotto 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, con evidenza che le istruzioni stesse sono integrabili dai singoli Referenti Privacy di afferenza attraverso ulteriori istruzioni di carattere specifico, anche per gruppi omogenei di funzioni.

Le istruzioni sono altresì integrate dalle puntuali disposizioni aziendali in materia di protezione dei dati personali (quali il Disciplinare sull'utilizzo dei Sistemi Informatici Aziendali e la procedura Dossier Sanitario elettronico) a cui si rinvia, reperibili sempre alla pagina Internet dedicata.

Si segnala al soggetto autorizzato che, per qualsiasi questione e/o approfondimento e/o chiarimento in materia di protezione dei dati personali può rivolgersi:

- al proprio **Referente Privacy** che, ai sensi dell'art. 3 del REGOLAMENTO PER IL TRATTAMENTO DEI DATI PERSONALI NELL'AZIENDA OSPEDALIERO UNIVERSITARIA DI FERRARA è il Direttore dell'Unità Operativa e/o il Dirigente titolare di strutture in staff alla Direzione alla quale si è assegnati;
- anche direttamente al **Responsabile della Protezione dei Dati Personali** (DPO), contattabile all'indirizzo email dpo@ospfe.it oppure, dall'interno dell'Azienda, al numero abbreviato 18486. Il DPO, in ogni caso, riceve il pubblico nel proprio ufficio sito in Via Aldo Moro n. 6 a Ferrara il mercoledi dalle 14 alle 18, ma solo previo appuntamento da concordare scrivendo a dpo@ospfe.it.

2. Glossario.

Dato personale: si intende qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

Dato personale di natura particolare (c.d. dato sensibile): si intendono i dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale nonché i dati genetici, i dati biometrici, i dati relativi alla salute alla vita sessuale, all'orientamento sessuale della persona, le condanne penali, i reati e le connesse misure di sicurezza.

Trattamento di dati personali: si intende qualunque operazione o complesso di operazioni, svolti con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati. In ogni caso l'elenco non è tassativo.

Titolare del trattamento: si intende l'intestata Azienda Sanitaria.

Soggetto autorizzato al trattamento: si intende il dipendente dell'Azienda o qualsiasi collaboratore, a qualsiasi titolo (libero professionista e/o lavoratore autonomo) autorizzato dall'Azienda al trattamento dei dati personali.

3. Principi Generali.

Il soggetto autorizzato è tenuto, nello svolgimento della propria attività, a:

1. trattare i dati di propria competenza nel rispetto dei principi di liceità, correttezza e trasparenza nonché del:

    a. 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;

b. principio di limitazione delle finalità: trattare i dati conformemente alle finalità istituzionali del Titolare, limitando il trattamento esclusivamente a dette finalità;

c. 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.

3. utilizzare le informazioni e i dati personali, in particolare i dati c.d. 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.

4. 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.

5. 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.

6. astenersi dal comunicare a terzi e/o a diffondere dati ed informazioni appresi in occasione dell'espletamento della propria attività.

7. 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 suo delegato.

4. Istruzioni operative per lo svolgimento delle operazioni caratterizzanti il trattamento.

Il soggetto autorizzato è tenuto, nello svolgimento della propria attività, a:

- identificazione degli interessati: nell'ambito dell'accesso alle prestazioni, l'autorizzato 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 deve essere fornita l'informativa 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;

- registrazione dei dati: non lasciare a disposizione di estranei supporti, fogli, cartelle e quant'altro;

- al momento della consegna di copie dei documenti ai destinatari è necessario adottare tutte le garanzie di sicurezza, quali l'utilizzo di buste sigillate e l'eventuale acquisizione della delega, se non è presente l'interessato, rispettando, comunque, le disposizioni previste dalla legge 219/2017 sulle modalità previste dalla normativa su come rendere note le informazioni sanitarie ai pazienti.

- In caso di **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 idonee a rivelare lo stato di salute dell'interessato o a creare una forma di associazione con una qualsivoglia patologia.

- i **documenti contenenti dati personali** (es. fogli di carta, cartelle cliniche, referti, prescrizioni, ecc.) devono essere custoditi in modo da non essere accessibili a persone non autorizzate. In particolare, i documenti contenenti dati sensibili devono essere controllati e custoditi in modo che non vi accedano persone prive di autorizzazione (es. custodia in cartelline non trasparenti, faldoni, dossier, armadi o cassetti chiusi a chiave, porte degli uffici chiuse a chiave od assicurate da altri dispositivi di chiusura elettronica, ecc.) e non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative;

- l'**archiviazione dei documenti cartacei** contenenti dati sensibili deve avvenire in locali ad accesso controllato, utilizzando armadi o cassetti chiusi a chiave. Per accedere agli archivi contenenti tali dati fuori orario di lavoro è necessario ottenere una preventiva autorizzazione da parte del proprio Referente, salvo che l'autorizzazione non sia già stata rilasciata;

- i documenti contenenti dati personali che vengono prelevati dagli archivi, correnti o storici, per l'attività quotidiana devono esservi riposti a fine giornata. Le **copie dei documenti** contenenti dati personali che risultino inutilizzate o mal riuscite non devono essere utilizzate come carta da appunti o da riciclo, e devono essere distrutte (non possono essere gettati negli ordinari porta rifiuti ma devono essere distrutti attraverso appositi apparecchi trita-documenti o distruggendo i supporti stessi in modo tale che non siano ricostruibili); in ogni caso le misure di sicurezza applicate alle copie o alle riproduzioni dei documenti contenenti dati personali devono essere identiche a quelle applicate ai documenti originali.

- i **documenti contenenti dati personali non devono rimanere incustoditi** su scrivanie o tavoli di lavoro. In particolare, nell'ipotesi di ricevimento di soggetti o terzi non autorizzati, i documenti eventualmente in utilizzo dovranno essere chiusi e nascosti alla vista dei soggetti non autorizzati, per evitare che questi possano carpire informazioni di soggetti contenuti in tali documenti.

- i fax pervenuti devono essere ritirati quanto prima; è **vietato l'invio di documenti contenenti dati personali a mezzo fax**. Laddove, su specifica disposizione aziendale, sia eccezionalmente stato consentito l'utilizzo del fax per invio di documenti contenenti dati personali, il soggetto autorizzato che procede all'invio deve precederlo chiamando il destinatario della comunicazione al fine di anticipare la trasmissione e di assicurare il ricevimento nelle mani del medesimo, evitando che soggetti o terzi non autorizzati conoscano il contenuto della documentazione inviata.

- è fatto divieto di effettuare **copie fotostatiche** e/o **stampe** o di qualsiasi altra natura se non richiesto ed autorizzato nell'ambito della propria mansione. In ogni caso il soggetto autorizzato che procedere alla copia e/o alla stampa di documenti è tenuto ad assicurarsi che l'originale e la copia vengano prelevate dalla fotocopiatrice e non lasciate in alcun modo incustodite.

- è fatto divieto di sottrarre, cancellare, distruggere senza l'autorizzazione del responsabile, stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del Trattamento, se non richiesto dalla propria mansione ed autorizzato nell'ambito della propria mansione.

- nelle comunicazioni telefoniche accertarsi sempre dell'identità del proprio interlocutore al fine di non divulgare dati a soggetti non autorizzati (l'identificazione può avvenire chiedendo all'interlocutore i suoi dati personali di non facile conoscenza quale, a titolo esemplificativo, il codice fiscale o l'indirizzo e-mail dallo stesso precedentemente comunicato).

Si segnala, in ogni caso, che il soggetto autorizzato è tenuto a procedere al trattamento nel rispetto di quanto previsto dal REGOLAMENTO PER IL TRATTAMENTO DEI DATI PERSONALI NELL'AZIENDA OSPEDALIERO UNIVERSITARIA DI FERRARA pubblicato al seguente link.

5. Istruzioni operative per il corretto utilizzo degli strumenti aziendali per il trattamento dei dati personali.

Il soggetto autorizzato è tenuto, nello svolgimento della propria attività, a:

- il codice identificativo personale e la password vengono assegnati dal Servizio Comune ICT, personalmente al soggetto autorizzato che, a tal fine, è obbligato a identificarsi. Al primo accesso il soggetto autorizzato deve modificare la propria password. Al fine di creare una password sicura si suggerisce di seguire le indicazioni contenute nel documento reperire al link.

- è fatto divieto di condividere il proprio codice identificativo e la propria password con altri. In particolare, la password non può essere comunicata a nessuno. A tali fini la password non può essere trascritta in supporti che ne consentirebbero o agevolerebbero la conoscenza da parte di terzi (es. post-it, trascrizione in supporti presenti sulla Sua scrivania). Se si ha il sospetto o il dubbio che taluno sia venuto accidentalmente o intenzionalmente a conoscenza della propria password è necessario modificarla con immediatezza e, in caso di impossibilità, avvisare il Servizio Comune ICT ai fini del suo reset.

- 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;

- Email e Internet: la posta elettronica e la rete Internet possono essere utilizzata solo per scopi di ufficio. Occorre prestare particolare attenzione alla spedizione, a mezzo di posta elettronica, di files o di messaggi contenti dati riferiti alla salute che, nel caso, devono essere criptati o possono essere effettuati esclusivamente attraverso il cloud aziendale.

- 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 attivare il "blocca schermo" anche se si è a conoscenza del fatto che decorso un certo periodo di tempo tale sistema si attiva in autonomia. Laddove non sia possibile procedere con tale modalità sarà necessario 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 altre 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 (un armadio o un cassetto chiusi a chiave, una cassaforte, ecc.).

- i **supporti rimovibili** di qualsivoglia natura per la registrazione di dati devono essere forniti dal Servizio Comune ICT e, nel caso in cui debbano essere distrutti, dovrà procedervi consegnandoli al medesimo Servizio; in ogni caso è fatto espresso divieto di salvare dati personali di qualsiasi natura in supporti esterni (es. chiavette USB, pc portabili, ecc.), così come di salvarli in servizi cloud e/o di inviarli via e-mail in violazione delle indicazioni contenute nelle presenti Istruzioni o delle istruzioni ricevute dal Servizio ICT;

- è fatto **divieto di inviare allegati e/o dati personali** di titolarità dell'Azienda tramite applicazioni di messaggistica e/o chat (es. **Whatsapp, Telegram, Signal**): a tal fine, al più, si consiglia di creare una cartella zip protetta da password, da inviare attraverso la casella di posta elettronica aziendale (o mediante condivisione dal cloud aziendale secondo le indicazioni reperibile al seguenti link. Fermo restando il diritto di utilizzare gli strumenti di messaggistica per finalità di mera comunicazione tra utenti, si segnala che detti strumenti non possono essere utilizzati per inviare comunicazioni e/o documenti inerenti l'attività aziendale.

Il soggetto autorizzato, in ogni caso, è tenuto a rispettare quanto previsto nel Disciplinare sull'utilizzo dei Sistemi Informativi Aziendali reperibile al seguente link.

6. Istruzioni riguardanti rapporti di Front Office o il trattamento dei dati in ambito sanitario.

Il soggetto autorizzato è tenuto, nello svolgimento della propria attività che riguardi rapporti a diretto contatto coi pazienti e/o, comunque con soggetti esterni, a:

- **rispettare e/o imporre alle predette persone fisiche la distanza di sicurezza/cortesia**: 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 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), chiedendo in formazioni che sono di agevole conoscenza dell'interlocutore stesso, ma avendo cura di chiederle senza suggerire la risposta.

- **evitare di ripetere ad alta voce i dati** che non è necessario ribadire. Anche nelle comunicazioni telefoniche è opportuno evitare di far conoscere ai presenti il nominativo della persona con cui si sta parlando;

- procedere alla **chiamata del paziente** utilizzando soluzioni che prevedano un ordine di precedenza e di chiamata degli interessati che prescinda dalla loro individuazione nominativa. In particolare i pazienti in attesa devono essere chiamati utilizzando, se esistente, il numero della prenotazione e/o il numero assegnato al momento dell'ingresso, avendo cura di indirizzarlo verso l'ambulatorio o il servizio indicato in modalità generica (es. il paziente dovrà essere indirizzato all'ambulatorio 3 e non all'ambulatorio "melanoma") ed evitando di chiedere alla presenza di altre persone la ragione della visita e/o la patologia e/o altre indicazioni capaci di far comprendere a terzi informazioni sanitarie dei paziente. I **pazienti minori di età** dovranno invece essere chiamati utilizzando il primo nome (senza chiamare il cognome, se non in caso di omonimia);

- il **trasporto di documentazione**: va fatto utilizzando le dovute cautele al fine di impedire un accesso non autorizzato (es. utilizzo di contenitori/buste sigillate, ecc.);

- la **consegna di documentazione sanitaria** deve essere fatta utilizzare buste sigillate, previo accertamento dell'identità del diretto interessato. La documentazione sanitaria può essere consegnata a persone diverse dall'interessato solo previa consegna di **delega sottoscritta** dall'interessato con allegazione della copia di un documento di identità e avendo cura di verificare la probabile riferibilità della sottoscrizione all'interessato stesso. Deve essere **identificato anche il consegnatario** chiedendo l'esibizione di un suo documento di identità.

- il **dialogo-colloquio tra personale dell'azienda e utenti** deve essere improntato ad un criterio di prudenza per cui si suggerisce di non dialogare di questioni sanitaria all'esterno dei luogi all'uopo deputati (es. nei corridoi). Anche i dialoghi, le visite o comunque qualsivoglia intervento sui pazienti all'interno di camere occupate da più persone deve avvenire avendo cura di invitare persone in visita ad uscire dalla stanza, chiudendo la porta e, comunque, avendo cura di non riferire informazioni particolarmente sensibili alla presenza di altri pazienti all'interno della stanza. Laddove sia necessario riferire al paziente informazioni delicate, lo stesso dovrà essere invitato a recarsi presso l'ambulatorio del medico per garantire la riservatezza e la segretezza della comunicazione.

[VER. 31/12/2022]