



ISTRUZIONI PER LE PERSONE AUTORIZZATE AL TRATTAMENTO DEI DATI PERSONALI

Nel presente documento sono riportate le istruzioni che Istituto Oncologico Veneto - IRCCS, in qualità di titolare del trattamento dei dati personali (di seguito, il "Titolare"), impartisce alle persone autorizzate a svolgere operazioni di trattamento sotto la sua autorità.

Operazioni di trattamento.

Al fine di evitare rischi di accesso non autorizzato o non consentito, perdita, distruzione o danneggiamento dei dati (anche accidentali), le persone autorizzate al trattamento dei dati personali devono attenersi a tutte le prescrizioni e misure di sicurezza che vengono qui di seguito riportate.

- 1) Controllare e custodire gli strumenti elettronici utilizzati per il trattamento dei dati e i documenti contenenti dati personali, di cui si è a conoscenza o in possesso per lo svolgimento delle attività e dei compiti assegnati, in modo tale da impedire l'accesso a persone non autorizzate o trattamenti non consentiti.
- 2) Curare la gestione delle credenziali d'autenticazione secondo le specifiche procedure ed istruzioni operative previste dai manuali e documenti aziendali, attenendosi inoltre alle seguenti disposizioni:
 - a) utilizzare il codice identificativo (user-id) e la password riservata assegnati per l'accesso ai dati trattati mediante strumenti elettronici e custodirli diligentemente garantendone la segretezza;
 - b) la password deve essere composta da una sequenza di almeno otto caratteri (normali e speciali) sia numerici che alfabetici (o, se il programma in uso non lo permetta, dal numero massimo di caratteri consentito);
 - c) nella generazione della password, si deve prestare la massima attenzione a non utilizzare elementi o notizie facilmente riconducibili all'utilizzatore. Devono quindi, ad esempio, essere evitati riferimenti a: nome e cognome, data di nascita, numero di matricola, nome di familiari, numero di telefono di casa o dell'ufficio, soprannomi noti, nonché nomi di personaggi famosi, ecc.;
 - d) la password deve essere modificata al primo utilizzo ed ogni volta che viene richiesto dal sistema (al massimo: 6 mesi per i dati personali e 3 mesi per quelli particolari¹), ovvero ogniqualvolta vi sia il dubbio che ne sia stata violata la segretezza. Nella generazione della nuova password, non devono essere utilizzate sequenze di caratteri già usate in precedenza;
 - e) la password deve rimanere assolutamente riservata. A tale fine, deve essere evitata la digitazione in presenza di terzi ed è necessaria la conservazione in luogo non accessibile ad altri (va dunque assolutamente evitata l'apposizione sul video-terminale di biglietti o adesivi contenenti riferimenti alla password). Va altresì evitato l'uso di sistemi automatici di inserimento di password (es. macro o predisposizione tasti funzione);
 - f) la password non può essere comunicata, per nessun motivo, ai colleghi del proprio o di altri uffici.
- 3) In tutti i casi di allontanamento, anche temporaneo, dalla postazione di lavoro (es: pausa pranzo), è necessario bloccare la propria sessione di lavoro. Tale accorgimento deve essere adottato soprattutto in caso di utilizzazione, da parte di più soggetti autorizzati, della medesima postazione di lavoro.
- 4) Tutte le persone autorizzate al trattamento dei dati devono partecipare attivamente agli eventuali interventi formativi in materia di privacy organizzati dal Titolare e devono riferire al responsabile dell'area/ufficio a cui è assegnato o, in mancanza, al delegato privacy eventualmente nominato o al legale rappresentante ogni e qualsiasi anomalia riscontrata nell'esercizio della propria attività.

¹ Si tratta delle seguenti categorie di dati: dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (art. 9 GDPR).



- 5) I trattamenti di dati contenuti in atti e documenti cartacei devono essere svolti garantendo sempre la corretta custodia degli stessi. I documenti non possono, pertanto, essere lasciati incustoditi sulla propria scrivania e/o in luoghi aperti al pubblico in assenza di altri soggetti autorizzati addetti al medesimo trattamento; non devono essere consultati da altri soggetti autorizzati non abilitati al trattamento; non possono essere riprodotti o fotocopiati se non per esigenze connesse alla finalità del trattamento; non possono essere portati al di fuori dei locali individuati per la loro conservazione se non in casi del tutto eccezionali e, qualora si procedesse in tal senso, l'asportazione dovrà essere ridotta al tempo minimo necessario per effettuare le operazioni di trattamento. Al termine dell'orario di lavoro, la persona autorizzata al trattamento deve, inoltre, riportare tutti i documenti cartacei contenenti dati personali nei locali individuati per la loro conservazione.
- 6) Qualora sia necessario distruggere i documenti cartacei contenenti dati personali, questi devono essere distrutti utilizzando gli appositi apparecchi "distruggi documenti" o, in assenza, devono essere sminuzzati in modo da non essere più ricomponibili.
- 7) È proibito comunicare dati personali per telefono, se non si è certi che il destinatario sia una persona autorizzata al trattamento dei dati personali in questione.
- 8) In tutte le ipotesi in cui venga utilizzata una stampante condivisa da vari utenti situata al di fuori dei locali ove è posta la singola stazione di lavoro, alle operazioni di stampa sarà possibile procedere soltanto previa verifica della assenza, nei locali ove è situata la stampante, di soggetti non autorizzati al trattamento. Le stampe devono essere raccolte immediatamente e custodite con le modalità descritte nei punti precedenti.
- 9) È fatto assoluto divieto di entrare in locali ad accesso limitato, se non previa espressa autorizzazione del relativo responsabile.
- 10) Qualora sia effettuato un trattamento di eventuali categorie particolari di dati personali e/o di dati personali relativi a condanne penali e reati, ogni persona autorizzata al trattamento è, inoltre, tenuta a:
 - a) custodire tutti i supporti rimovibili su cui sono memorizzati eventuali categorie particolari di dati personali e dati personali relativi a condanne penali e reati (usb pen drive, dvd rom, cd rom, ecc.) in modo da evitare accessi e trattamenti non autorizzati;
 - b) distruggere i suddetti supporti rimovibili al termine del loro utilizzo, ovvero cancellare definitivamente le informazioni in essi registrate prima di un loro riutilizzo;
 - c) custodire i documenti contenenti particolari di dati personali e dati personali relativi a condanne penali e reati in archivi chiusi a chiave e limitandone l'accesso alle sole persone preventivamente autorizzate;
 - d) restituire i documenti contenenti tali dati al termine delle operazioni di trattamento ai soggetti incaricati della relativa archiviazione.

Riscontro alle istanze per l'esercizio dei diritti.

- 1) La persona autorizzata al trattamento che riceva l'istanza deve darne comunicazione immediatamente (e comunque entro la stessa giornata) al responsabile dell'area/ufficio a cui è assegnato o, in mancanza, al delegato privacy eventualmente nominato o al legale rappresentante.
- 2) Al responsabile della struttura/ufficio di riferimento o, in mancanza, al delegato privacy eventualmente nominato o al legale rappresentante, competono i seguenti obblighi, che osserverà eventualmente con la collaborazione della persona autorizzata che ha raccolto l'istanza:
 - a. accertare l'ammissibilità della richiesta;
 - b. qualora sussistano ragionevoli dubbi circa l'identità della persona fisica che presenta l'istanza, dovranno essere richieste ulteriori informazioni necessarie per confermare l'identità dell'interessato, in particolare chiedendo l'esibizione di un documento d'identità del richiedente o la trasmissione di copia dello stesso, a meno che non si tratti di persona già conosciuta;



Regione del Veneto
Istituto Oncologico Veneto
Istituto di Ricovero e Cura a Carattere Scientifico



REGIONE DEL VENETO

- c. nel caso di richiesta presentata da un terzo per conto dell'interessato, acquisire copia della delega o procura sottoscritta dall'interessato, che dovrà essere presentata unitamente a copia di un documento d'identità dell'interessato e a copia di un documento d'identità del delegato;
- d. concluse positivamente le fasi sopra descritte, verificare il trattamento dei dati personali oggetto della richiesta al fine di evaderla tempestivamente. In particolare, in caso di esercizio del diritto di accesso occorrerà individuare i dati personali richiesti presso gli archivi elettronici e/o cartacei di interesse, estrapolarli ed inserirne copia su apposito supporto elettronico o cartaceo, se necessario, nonché provvedere all'invio all'interessato al recapito dallo stesso indicato con modalità che permettano di assicurare un'adeguata documentazione di tale invio e, se possibile, della ricezione da parte dell'interessato. In relazione all'esercizio degli altri diritti sarà necessario procedere nei termini che seguono: qualora la richiesta fosse fondata, dovrà essere data chiara e specifica attestazione dell'intervento effettuato (*es.: avvenuta rettifica o cancellazione dei dati contestati*); in caso contrario, dovrà essere dato atto delle motivazioni per le quali non è stato possibile il riscontro.

Indicazioni generali:

- alla richiesta deve essere fornito riscontro entro un mese, che in casi di particolare complessità potrà essere estendibile al massimo di ulteriori due mesi: entro un mese dalla ricezione della richiesta, deve comunque essere dato riscontro all'interessato;
- qualora la richiesta fosse inammissibile o infondata, il mittente dovrà essere informato dei motivi dell'inottemperanza e della possibilità di proporre reclamo a un'autorità di controllo o di proporre ricorso giurisdizionale: tale comunicazione dovrà essere inoltrata senza ritardo e comunque entro un mese dal ricevimento della richiesta;
- l'esercizio dei diritti è generalmente gratuito: a fronte di richieste manifestamente infondate, eccessive o ripetitive, tuttavia, può essere stabilito l'ammontare del contributo da chiedere in ragione della complessità del riscontro; inoltre, qualora fossero richieste ulteriori copie dei dati personali oggetto di trattamento potrà essere addebitato un contributo spese ragionevole, basato sui costi amministrativi sostenuti.

Data ultimo aggiornamento: 12.09.2019