

Allegato 2 - T04/IOS01

ISTRUZIONI di CARATTERE GENERALE impartire dal Titolare a tutti i SOGGETTI AUTORIZZATI AL TRATTAMENTO DEI DATI PERSONALI

Principi Generali

1. Trattare i dati di propria competenza nel rispetto dei principi di liceità, correttezza e trasparenza.
2. In attuazione 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.

Istruzioni operative

ISTRUZIONI PER LO SVOLGIMENTO DELLE OPERAZIONI CARATTERIZZANTI IL PROCESSO DI TRATTAMENTO

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

ISTRUZIONI PER IL CORRETTO UTILIZZO DEGLI STRUMENTI AZIENDALI PER IL TRATTAMENTO DEI DATI PERSONALI

- 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 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. A tal specifico fine si rinvia alle disposizioni aziendali (es. IOA29, IOA44, istruzioni operative per l'utilizzo della posta elettronica e internet ecc.....)
- 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 (un armadio o un cassetto chiusi a chiave, una cassaforte, ecc.).

ISTRUZIONI RIGUARDANTI RAPPORTI DI FRONT OFFICE

- 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 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).

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.

Le suddette istruzioni sono integrabili dai singoli Referenti Privacy di afferenza attraverso ulteriori istruzioni di carattere specifico, anche per gruppi omogenei di funzioni.

Le istruzioni di cui sopra sono altresì integrate dalle puntuali disposizioni aziendali in materia di protezione dei dati personali:

1. *Istruzione operativa per il corretto utilizzo dei sistemi informatici aziendali (IOA44);*
2. *Manuale Operativo sull'utilizzo del Dossier Sanitario elettronico;*
3. *Istruzione Operativa sull'utilizzo della posta elettronica e internet*

a cui si rinvia, reperibili sempre alle pagine intranet dedicate <https://intranet.aosp.bo.it/content/la-privacy-azienda> e http://qweb.aosp.bo.it/cgi-bin/isopubb/isopubb_gestione?search.