

Istruzioni aziendali ai responsabili e agli incaricati per lo svolgimento delle operazioni di trattamento

Premesse

I trattamenti, di cui è titolare l'Azienda USL di Piacenza (di seguito denominata azienda), possono essere di tre specie e di conseguenza riguardare tre livelli:

- a) trattamenti che riguardano finalità istituzionali dell'Azienda, conosciuti e monitorati dai responsabili dei sistemi informativi. Sono trattamenti che, nella maggior parte dei casi, sono caratterizzati dalla trasversalità e che possono, di conseguenza, coinvolgere più di una Unità Operativa;
- b) trattamenti svolti in seno alle singole unità operative (responsabili del trattamento), che non sono oggetto di specifico monitoraggio da parte del responsabile dei sistemi informativi, o che vengono svolti utilizzando strumenti non automatizzati. In questo caso i responsabili del trattamento devono rispettare i principi generali, caratterizzanti ogni singolo trattamento, di seguito specificati;
- c) infine, attività di trattamento che sono svolte dai singoli responsabili, per scopi non incompatibili con le finalità istituzionali dell'azienda e con quelle dichiarate agli interessati in sede di informativa, fornita al momento della raccolta dei dati medesimi (l'esempio può essere rinvenuto nel trattamento dei dati di un paziente, effettuato da un medico, per scopi di ricerca scientifica).

Con riferimento ai trattamenti considerati alle lettere precedenti, gli ordini di profili che bisogna considerare sono i seguenti:

- **la titolarità:** il d. lgs. 196/2003 (di seguito denominato "codice privacy") definisce il titolare del trattamento come il soggetto cui spetta definire le finalità e le modalità del trattamento, gli strumenti e le misure di sicurezza. La titolarità del trattamento, nel caso di una pubblica amministrazione, è dell'ente nel suo complesso, che la esercita attraverso il suo legale rappresentante;
- **la gestione del trattamento o delle eventuali banche dati:** la gestione è profilo diverso dalla titolarità; a tal proposito l'azienda titolare del trattamento ha nominato, quali responsabili del trattamento, i Dirigenti Responsabili pro-tempore delle UU.OO. complesse e UU.OO. semplici dipartimentali espressamente individuate.
- **il monitoraggio dei trattamenti:** quest'ultimo aspetto attiene alla verifica della sussistenza degli elementi che caratterizzano i trattamenti; in particolare: la finalità, le modalità del trattamento, l'eventuale costituzione e detenzione di una banca dati, la natura dei dati trattati, le misure di protezione adottate.

Ogni responsabile, secondo quanto previsto dalla legge, nel procedere al trattamento dei dati personali, in seno alla propria unità di appartenenza, deve rispettare i seguenti principi:

- 1) principio di finalità (art. 11 lettera b) del codice privacy): il trattamento deve essere svolto per scopi determinati, espliciti e legittimi. Ciò vale a maggior ragione per i soggetti pubblici, che possono procedere al trattamento in applicazione del principio di finalità istituzionale, senza dover richiedere il consenso dell'interessato al trattamento, salvo il caso previsto dall'art. 76 del codice privacy, con specifico riferimento ai dati idonei a rivelare lo stato di salute trattati per finalità di tutela della salute o dell'incolumità fisica dell'interessato;
- 2) principio di proporzionalità (art. 11 lettera d) del codice privacy): i dati, oggetto di trattamento, devono essere pertinenti, non eccedenti e completi rispetto agli scopi, di cui alla lettera precedente;
- 3) principio di sicurezza (articoli 31 e seguenti del codice privacy): i dati oggetto di trattamento devono essere protetti attraverso l'adozione di misure di sicurezza.

ISTRUZIONI

Di seguito vengono specificate le regole che i singoli responsabili sono tenuti ad osservare e a far rispettare ai propri incaricati del trattamento:

a) istruzioni per lo svolgimento delle operazioni caratterizzanti il processo di trattamento:

obbligo di riservatezza e segretezza: deve essere mantenuta l'assoluta segretezza sulle informazioni di cui si venga a conoscenza nel corso delle operazioni del trattamento e si deve evitare qualunque diffusione delle informazioni stesse. Si ricorda che l'eventuale violazione dell'obbligo ivi considerato può comportare l'applicazione di sanzioni di natura disciplinare ed una responsabilità civile e penale, secondo quanto previsto dal codice della privacy;

occorre far rispettare le **distanze di sicurezza:** per quanto riguarda gli operatori di sportello (cd. front-office) deve essere prestata attenzione al rispetto dello spazio di cortesia e se del caso invitare gli utenti a sostare dietro la linea tracciata sul pavimento ovvero dietro le barriere delimitanti lo spazio di riservatezza;

raccolta: prima di procedere alla raccolta dei dati personali, deve essere fornita **l'informativa all'interessato** o alla persona presso cui si raccolgono i dati, secondo quanto stabilito dall'art. 13 del codice privacy (in forma orale oppure utilizzando apposita modulistica predisposta dal Titolare); occorre inoltre **procedere alla raccolta dei dati con la massima cura** verificando l'esattezza dei dati stessi;

registrazione: non lasciare dischetti, fogli, cartelle e quant'altro a disposizione di estranei;

conservazione: i documenti o gli atti che contengono dati sensibili o giudiziari devono essere conservati in archivi ad accesso controllato. A titolo meramente esemplificativo, un accesso può dirsi "controllato" nel caso in cui armadi, schedari, contenitori in genere siano muniti di serratura, ovvero siano soggetti a sorveglianza da parte di un presidio umano all'interno della stanza, o del luogo di conservazione dei dati, tale da consentire un controllo sulla identità di coloro che hanno accesso all'archivio considerato. Sarà cura di ogni singolo responsabile del trattamento, chiamato ad adottare le misure minime di sicurezza, provvedere affinché venga escluso un accesso ad archivi e a dati da parte di soggetti che non siano incaricati del trattamento;

utilizzo: i dati possono essere utilizzati solo da coloro che sono stati espressamente incaricati al trattamento, che dovrà avvenire solo per scopi determinati, espressi e legittimi;

blocco: questo può essere conseguenza di una espressa richiesta da parte dell'interessato ovvero può essere ordinato dal Garante per la protezione dei dati personali;

comunicazione: per comunicazione, secondo quanto previsto dalla legge, si intende "il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione". Ciò che caratterizza l'operazione di comunicazione è il fatto che stante il rapporto diretto tra titolare (Azienda sanitaria) e interessato, un soggetto determinato (in posizione di terzietà rispetto a questi due soggetti) possa in qualunque forma conoscere dati personali riferiti all'interessato medesimo;

comunicazione di dati cd. comuni: con questa espressione si intendono i dati personali diversi da quelli espressamente individuati dal codice e definiti come dati sensibili o giudiziari (cfr. articolo 4, comma 1 lettere d) ed e). La comunicazione di questa tipologia di dati personali può avvenire solo se espressamente prevista da una legge o da un regolamento. Qualora il richiedente i dati personali sia un soggetto pubblico, la comunicazione dei cd. dati comuni potrà avvenire, pur in mancanza di espressa previsione di legge o di regolamento, ove sia necessaria per l'esercizio di una finalità istituzionale dell'ente destinatario della comunicazione stessa;

comunicazione di dati sensibili: i dati sensibili, espressamente individuati dall'art. 4, lett. d) del codice privacy (dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose,

filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale), possono essere comunicati a soggetti determinati solo ove sia espressamente previsto da una legge, che autorizzi tale operazione, ovvero da un regolamento ad efficacia esterna. La comunicazione dei dati all'interessato deve avvenire, di regola, direttamente a quest'ultimo o ad un suo delegato, in plico chiuso o con altro mezzo idoneo a prevenire la conoscenza da parte di soggetti non autorizzati. Secondo quanto previsto dall'art. 76 del codice, i dati idonei a rivelare lo stato di salute possono essere trattati (e di conseguenza oggetto di comunicazione a terzi) con il consenso scritto dell'interessato, solo ed esclusivamente nel caso in cui il trattamento sia necessario per una finalità di tutela della salute e dell'incolumità fisica dell'interessato medesimo;

rilascio delle copie di documentazione sanitaria: il rilascio di copia di documentazione sanitaria (tra cui nello specifico delle cartelle cliniche) è disciplinato dall'articolo 92 del codice privacy. Considerata la natura dei dati contenuti in detti documenti, sia i Responsabili, sia gli incaricati del trattamento dovranno attenersi alle procedure specificatamente definite dalla Direzione Amministrativa di Rete Ospedaliera e dalle Direzioni Sanitarie.

diffusione: per diffusione si intende "il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione". La pubblicazione delle deliberazioni e delle determinazioni, qualora le stesse contengano dati personali, costituisce, ai sensi della normativa sulla privacy, una forma di diffusione di informazioni personali. Si ricorda che l'art. 22, comma 8 del codice privacy vieta espressamente la diffusione di dati personali idonei a rivelare lo stato di salute. Sarà cura quindi dei soggetti che redigono gli atti oggetto di pubblicazione di far sì che si rispetti il divieto considerato. Dovrà pertanto essere predisposta la copia degli atti deliberativi da pubblicare, in una forma in cui vi sia il testo della stessa corredato da allegati; questi ultimi, contenenti i dati sanitari, non dovranno essere oggetto di pubblicazione, ma dovranno rimanere agli atti, conservati secondo quanto previsto dalla legge, e a disposizione di coloro che abbiano la legittimazione all'esercizio del diritto di accesso, secondo quanto previsto dalla legge n. 241/90;

cancellazione: i dati personali, una volta che sia stato raggiunto lo scopo del trattamento, non devono essere conservati in una forma che consenta l'identificazione dell'interessato. Si tratta del cd. diritto all'oblio previsto dall'art. 11, lettera e) del codice privacy. Tuttavia, il trattamento dei dati per scopi storici, di ricerca scientifica o di statistica è compatibile con gli scopi per i quali i dati sono raccolti o successivamente trattati e può essere effettuato anche oltre il periodo necessario a questi ultimi scopi;

distruzione dei dati: valgono le considerazioni svolte al punto precedente. Inoltre, i documenti cartacei, non più utilizzati, devono essere distrutti o comunque resi illeggibili, prima di essere eliminati o cestinati;

b) istruzioni per il corretto utilizzo degli strumenti per il trattamento:

computer: uscire dal programma in uso quando non sia più utilizzato. Tutte le volte che si abbandona la propria postazione di lavoro i pc e/o i terminali devono essere posti in condizione da non essere utilizzati da estranei. Qualora si dovessero riscontrare delle violazioni al principio di proporzionalità (ossia non pertinenza, eccedenza o incompletezza dei dati, rispetto agli scopi del trattamento), il responsabile dovrà prontamente procedere alla loro modificazione, integrazione o rettificazione, ovvero alla loro cancellazione, quest'ultima ipotesi nel caso in cui il trattamento avvenga in violazione della legge;

e-mail e uso dell'Internet: la posta elettronica può essere utilizzata per scopi d'ufficio. Occorre fare particolare attenzione alla spedizione, a mezzo di posta elettronica, di file o di messaggi contenenti dati sensibili. In tal caso, occorrerà proteggere il contenuto del file dall'accesso e dalla visione di soggetti, non autorizzati o legittimati al trattamento, che siano diversi dai destinatari delle comunicazioni elettroniche considerate. Tramite il ricorso all'uso di tecniche di criptazione o di cifratura dei messaggi, ovvero ricorrendo all'uso di codificazione dei dati contenuti nel testo delle comunicazioni. In particolare, per codificazione si intende la sostituzione dei dati identificativi dell'interessato con codici alfanumerici, ovvero qualsiasi tecnica, che sia utile a far venir meno il

legame tra l'identità del soggetto interessato ed una o più condizione idonea ad identificare una delle qualità espressamente previste dall'art. 4, comma 1 lettera d);

telefono e fax: non fornire dati e informazioni di carattere sanitario per telefono, qualora non si abbia la certezza assoluta sull'identità del soggetto chiamante; qualora giungano richieste telefoniche di dati sanitari da parte dell'Autorità Giudiziaria o degli organi di polizia e, in ogni caso, nell'ipotesi di richieste di comunicazione di dati presentate per telefono o per fax occorre verificare preliminarmente l'identità del soggetto richiedente. Prima di inviare via fax documenti contenenti dati sensibili o comunque per i quali vi siano particolari esigenze di riservatezza, assicurarsi preventivamente che l'effettivo destinatario sia sul posto o comunque che non vi siano rischi di conoscenza del contenuto da parte di soggetti non autorizzati. Sulla copertina del fax, che viene utilizzata per la spedizione della documentazione allegata, che contenga dati personali riferiti a terzi, si deve 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";

floppy-disk: i **supporti informatici**, già utilizzati per il trattamento dei dati sensibili e giudiziari, **possono essere riutilizzati solo se le informazioni precedentemente contenute non sono più in alcun modo recuperabili**, dovendo **altrimenti** essere **distrutti**. Tali dispositivi, qualora contengano dati personali, devono essere conservati in contenitori muniti di serratura;

cd-rom: i **supporti informatici**, già utilizzati per il trattamento dei dati sensibili e giudiziari, **possono essere riutilizzati solo se le informazioni precedentemente contenute non sono più in alcun modo recuperabili**, dovendo **altrimenti** essere **distrutti**. Tali dispositivi, qualora contengano dati personali, devono essere conservati in contenitori muniti di serratura;

spedizione di documenti contenenti dati personali a mezzo posta: la documentazione contenente dati sensibili o giudiziari dovrà avvenire in busta chiusa. In alcuni casi, può essere utile utilizzare una busta non intestata, al fine di garantire la riservatezza del destinatario, qualora la corrispondenza venga recapitata a terzi, o comunque si abbia il dubbio che il destinatario possa vedere lesa la propria sfera di riservatezza, anche con il solo riferimento alla natura del mittente;

trasferimento di documenti cartacei all'interno dell'ente: qualora la documentazione contenga dati sensibili, i flussi documentali all'interno dell'ente devono avvenire nel rispetto della riservatezza degli interessati e adottando misure che siano idonee a limitare la conoscenza dei dati medesimi da parte dei soli soggetti destinatari;

uso di software: è vietato installare e usare qualunque software, anche se scaricato da internet, senza la previa autorizzazione da parte del responsabile del trattamento. Si ricorda che l'uso di software contraffatto, ovvero senza licenza d'uso, costituisce un illecito, sia di natura penale, sia civile, secondo quanto previsto dalla legge sul diritto d'autore (legge n. 633/1941), così come integrata dal d. lgs. n. 518/1992 e successive modificazioni e integrazioni;