AZIENDA USL DI RIMINI

ISTRUZIONI AGLI INCARICATI INTERNI

❑ Definizione

Per *INCARICATI INTERNI* si intende i dipendenti dell'Azienda USL di Rimini, consulenti e personale esterno con qualsiasi rapporto di collaborazione continuativo che, per il tipo di attività che svolgono, preveda l'accesso continuo alle strutture dell'Azienda.

❑ CONSERVAZIONE DI BANCHE DATI PERSONALI

Le Banche Dati devono essere custodite in modo da garantire la sicurezza dei dati in esse contenute, evitandone la divulgazione, la perdita, la distruzione e l'uso improprio.

➢ Sarà opportuno assicurarsi che l'ufficio in cui sono conservate le banche dati sia custodito durante l'orario di apertura

➢ Fuori orario di apertura o comunque in assenza di personale:

- le banche dati se su supporto cartaceo o su floppy disk dovranno essere custodite in armadi/locali chiusi a chiave
- le banche dati correnti (es. cartelle cliniche dei pazienti in corso di ricovero) devono essere rese accessibili solo al personale che abbia reali esigenze di accesso (es. personale di altro reparto ospedaliero che ha ragioni di assistenza e cura del paziente medesimo)
- nel caso in cui per ragioni logistiche ed organizzative non sia possibile conservare le banche dati in luoghi chiusi, la presenza di personale in orario di servizio e con continuità nell'arco della giornata dovrà essere garanzia di vigilanza

➢ **Cartelle Cliniche**

Le cartelle cliniche, all'avvio della procedura Medtrak nei reparti, vengono inserite in contenitori a cartella recanti il nome e cognome del paziente ed un codice a barre identificativo del paziente stesso. Durante i percorsi all'interno dell'ospedale la responsabilità della cartella clinica del paziente, racchiusa dentro l'apposito contenitore, è in capo all'ausiliario che trasporta il paziente. All'arrivo nel reparto di destinazione, la cartella deve essere affidata agli infermieri del reparto che ne assumono la responsabilità quanto alla custodia.

➢ ***Custodia delle cartelle cliniche***

Le cartelle cliniche dei pazienti in corso di ricovero sono contenute negli appositi carrelli.
Tali carrelli devono, di norma, essere custoditi in locali, il cui accesso è interdetto al pubblico (sarebbe ad esempio opportuno predisporre appositi cartelli all'ingresso di detti locali).
Se i carrelli contenenti le cartelle cliniche stazionano in locali non presidiati ventiquattro ore su ventiquattro ed i luoghi sono accessibili al pubblico in determinate fasce orarie occorre:

- se i locali sono presidiati durante l'accesso, fare in modo che alcuno consulti le cartelle cliniche e chiudere a chiave i locali oltre l'orario di accesso al pubblico
- se i locali non sono presidiati durante l'accesso al pubblico, riporre le cartelle cliniche in armadi con chiusura a chiave

- **COMUNICAZIONE DATI**

➢ ***Informazioni al pubblico***

La portineria può fornire a parenti e conoscenti informazioni sui pazienti ricoverati presso la struttura ospedaliera, senza tuttavia indicare il motivo del ricovero né la patologia.
Il programma MedTrak sarà predisposto in modo tale che in portineria non possa accedersi ad altra informazione se non a quella relativa al reparto di degenza.
Inoltre, nel caso in cui il degente abbia espresso la volontà di non rendere nota la sua presenza all'interno del presidio ospedaliero, tale informazione dovrà essere inserita nel programma MedTrak, onde consentire agli operatori della portineria la conoscenza della volontà espressa dal paziente. In tal caso apparirà il messaggio di non fornire alcuna indicazione a terzi.

➢ **Comunicazione all'interno dell'Azienda**

La comunicazione di dati personali e/o sensibili fra le strutture interne dell'Azienda deve avvenire nel rispetto del principio di finalità e pertinenza. Ciò significa che occorre trasmettere ma anche trattare solo i dati necessari alla **finalità** per cui sono stati richiesti.

➢ **Comunicazioni al di fuori dell'Azienda**

La comunicazione dei dati personali e/o sensibili deve essere effettuata nel rispetto dei generali principi di pertinenza del dato e non eccedenza rispetto alle finalità del trattamento e nel rispetto dei principi e delle regole di cui all'art. 84 del D.Lgs. 196/2003 che recita:

1. I dati personali idonei a rivelare lo stato di salute possono essere resi noti all'interessato da parte di esercenti le professioni sanitarie ed organismi sanitari, solo per il tramite di un medico designato dall'interessato o dal titolare. Il presente comma non si applica in riferimento ai dati personali forniti in precedenza dal medesimo interessato.

2. Il titolare o il responsabile possono autorizzare per iscritto esercenti le professioni sanitarie diversi dai medici, che nell'esercizio dei propri compiti intrattengono rapporti diretti con i pazienti e sono incaricati di trattare dati personali idonei a rivelare lo stato di salute, a rendere noti i medesimi dati all'interessato o ai soggetti di cui all'articolo 82, comma 2 lettera a). L'atto di incarico individua appropriate modalità e cautele rapportate al contesto nel quale è effettuato il trattamento di dati.

La comunicazione dei dati all'Autorità Giudiziaria

Il D.Lgs. 196/03 ha previsto alcuni principi applicabili al trattamento dei dati effettuato "da soggetti pubblici per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione dei reati, in base ad espresse disposizioni di legge che prevedano specificatamente il trattamento".
Dunque in questi casi la richiesta motivata ad esempio di un ufficiale di Polizia Giudiziaria che a seguito di sinistro stradale richiede di acquisire i giorni di prognosi dell'infortunato deve essere evasa.
Nel disciplinare, infatti, i casi di comunicazione la legge sulla privacy ha preso in considerazione la finalità di prevenzione, repressione e accertamento di reati così l'art. 21 recita:

- il trattamento di dati giudiziari da parte di soggetti pubblici è consentito solo se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichino le finalità di rilevante interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili.

La trasmissione dei dati mediante posta, all'interno o all'esterno dell'Azienda, dovrà avvenire sempre mediante supporti (cartacei, magnetici, ecc...) confezionati in buste o pacchi chiusi. Qualora non sia materialmente possibile eseguire tale procedura occorre porre in essere misure tali da garantire la sicurezza dei dati trasmessi e/o comunicati. Nel caso di dati personali "sensibili", sulla confezione o su un documento accompagnatorio, deve essere indicata la dicitura DATI RISERVATI, ed essere correttamente individuato il servizio destinatario. Tali modalità sono ancora più cogenti se i destinatari non fanno parte dell'Azienda.

Relativamente ai dati trasmessi via fax, il mittente ha l'onere di accertarsi con certezza il luogo di ricevimento del fax (es. che non sia un corridoio non presidiato) e nel caso si tratti luogo aperto, dovrà accertare la presenza del responsabile individuato.

Onde evitare accessi impropri ai dati personali è opportuno elaborare gli stessi al riparo da sguardi indiscreti, soprattutto allorché si tratti di dati sensibili.

☐ MISURE PER LA SICUREZZA DEI DATI TRATTATI CON STRUMENTI AUTOMATIZZATI

1. Gli utenti devono accedere solo ed esclusivamente alle risorse ed ai dati necessari per l'espletamento del proprio lavoro.

2. L'Azienda USL di Rimini vieta tassativamente la duplicazione abusiva dei programmi, ogni programma è infatti tutelato dalla legge sul diritto d'autore e ogni sfruttamento (duplicazione, commercializzazione, modificazione,....) dello stesso deve essere espressamente autorizzato dal titolare dei diritti esclusivi, fatto salvo i programmi di pubblico dominio o i programmi per i quali e permessa la duplicazione nei modi definiti dalla licenza.

3. L'Azienda USL di Rimini vieta tassativamente la riproduzione o la duplicazione con qualsiasi mezzo e a qualsiasi titolo dei manuali a corredo dei programmi, fatto salvo i manuali di pubblico dominio o i manuali per i quali e permessa la duplicazione nei modi definiti dalla licenza.

4. L'Azienda USL di Rimini permette, anzi incoraggia, così come previsto dall'art. 64-ter della legge 633/41, la predisposizione di copie di riserva dei programmi dotati di regolare licenza allo scopo di prevenire accidentali perdite dell'originale e quindi danni patrimoniali all'Azienda.
   Tali copie dovranno essere mantenute in appositi contenitori che le preservano da possibili furti.

5. L'Azienda USL di Rimini permette, anzi incoraggia, la realizzazione di copie di sicurezza degli archivi e dei dati che utilizzano applicativi di produttività personale, come gli strumenti di Office della Microsoft e comunque residenti sul proprio personal computer (non gestiti centralmente dall' U.O. Tecnologie Informatiche e di Rete), al fine del ripristino e quindi recupero di informazioni nel caso in cui il sistema, per motivi tecnici si blocchi e non possa rendere disponibili agli interessati che ne fanno richiesta le informazioni.

6. L'Azienda Usl di Rimini vieta tassativamente l'introduzione di virus o software maligno che pregiudichi il corretto funzionamento degli elaboratori e dei programmi dell'Azienda stessa.

7. L'Azienda USL di Rimini vieta tassativamente l'introduzione e l'installazione di applicativi e di dati provenienti dall'esterno dell'Azienda stessa se non a seguito di richiesta concordata con il Direttore della U.O. di appartenenza e presentata esclusivamente per fini di lavoro e comunque sotto la propria responsabilità riguardo il diritto d'autore di tali software. Tale richiesta va presentata al Responsabile di competenza del Trattamento dei dati che dovrà autorizzare previo accordo con il Responsabile della U.O. Tecnologie Informatiche e di Rete.

8. Le regole per l'utilizzo della parola chiave (password) per accedere ai programmi informatici dell'Azienda USL di Rimini sono le seguenti:

   - Ogni utente è responsabile della propria parola chiave.
   - E' vietato rivelare a qualsiasi persona (familiari, amici, conoscenti anche non dipendenti dell'Azienda USL di Rimini) la parola chiave per accedere ai programmi e quindi alle informazioni dell'Azienda.
   - E' bene modificare periodicamente la propria parola chiave.
   - E' obbligo utilizzare parole chiave lunghe 8 caratteri.
   - E' tassativamente vietato utilizzare applicativi identificandosi con la parola chiave di altri utilizzatori.
   - Non è consentito rivelare neanche ai tecnici, dipendenti o fornitori la propria password; essi per compiere operazioni sul sistema hanno una propria password assegnata per eseguire operazioni tecniche. Nel caso fosse necessario rivelare La propria parola chiave per rendere possibile un intervento tecnico, è fatto obbligo al titolare

di vigilare affinchè non ne venga fatto un uso improprio, nonché di modificare la parola chiave subito dopo l'esecuzione dell'intervento.

9. Occorre controllare le operazioni svolte dai fornitori di sistemi hardware e software, autorizzati ad eseguire operazioni all'interno dell'Azienda USL di Rimini, i quali utilizzano gli elaboratori degli utenti stessi. Se le operazioni si protraggono oltre l'orario di lavoro del dipendente occorre avvertire il responsabile della propria unità operativa.

10. Se ci si deve assentare dalla propria postazione di lavoro occorre prendere tutte le precauzioni possibili affinchè nessuno possa vedere le informazioni che appaiono a video o possa entrare nella rete aziendale sfruttando il fatto che l'utente è già connesso con la password del dipendente che ha acceso il computer ed eseguito le procedure di identificazione (Nome Utente e Password). Per questo può essere utile uscire dal programma utilizzato prima di assentarsi, in questo modo nessuno può vedere i dati visualizzati oppure eseguire funzioni per vedere le informazioni gestite dall'applicativo; spegnere il computer se si provvede ad assentarsi diverse ore e se si è sicuri che nussun altro utente debba condividere le risorse del proprio computer (Stampanti, disco rigido, ecc....); inserire il "salva schermo" protetto da password (modalità consigliata), in questo modo nessuno può utilizzare l'applicativo in uso, né utilizzare le funzioni e le risorse dell'elaboratore per entrare nella rete dell'Azienda.

11. Non è permesso il riutilizzo di un supporto magnetico floppy disk già contenente dati sensibili perché sono possibili comunque procedure di recupero di tali informazioni. Se per qualunque motivo è necessario cancellare i dati sensibili su floppy disk occorre eseguire la funzione di "formattazione completa" del supporto magnetico.

Si riporta infine il disposto dell'art. 15 del D.P.R. 10 Gennaio 1957 n. 3 "Statuto degli impiegati civili dello Stato" che recita:

1. L'impiegato deve mantenere il segreto d'ufficio. Non può trasmettere a chi non ne abbia diritto informazioni riguardanti provvedimenti od operazioni amministrative, in corso o concluse, ovvero notizie di cui sia venuto a conoscenza a causa delle sue funzioni, al di fuori delle ipotesi e delle modalità previste dalle norme sul diritto di accesso. Nell'ambito delle proprie attribuzioni, l'impiegato preposto ad un ufficio rilascia copie ed estratti di atti e documenti di ufficio nei casi non vietati dall'ordinamento.

Il Decreto Legislativo 196/03: "Codice in materia di protezione dei dati personali", riprendendo ed estendendo questi principi, testualmente sancisce all'art. 83 comma i):

" La sottoposizione degli incaricati che non sono tenuti per legge al segreto professionale a regole di condotta analoghe al segreto professionale".