All. 1

SISTEMA SANITARIO REGIONALE ASL ROMA 2	PRIVACY ASL ROMA 2	Revisione n. 1 02/2016	REGIONE LAZIO

REGOLAMENTO AZIENDALE SULLA PRIVACY -LE MISURE DI SICUREZZA -

Per misure di sicurezza deve intendersi l'insieme delle prescrizioni di carattere tecnologico, procedurale ed organizzativo finalizzate all'implementazione di un adeguato livello di sicurezza nel trattamento dei dati.

1. CRITERI TECNICI ED ORGANIZZATIVI PER LA PROTEZIONE DELLE AREE E DEI LOCALI

I dati e le informazioni di carattere sensibile e/o giudiziario devono essere trattati in aree protette, anche fisicamente, dall'accesso di persone non autorizzate. Sono perciò individuati spazi, dotati di un sistema di controllo all'ingresso e di eventuali sbarramenti di sicurezza. Un livello di protezione più elevato deve attivarsi per gli ambiti di trattamento e/o conservazione dei dati sensibili e giudiziari e ove sono ubicati i server di residenza dei dati e delle informazioni. Le barriere fisiche, ove necessario, devono essere configurate in modo tale da impedire l'accesso alle persone non autorizzate. Quando restano vuote, le aree di sicurezza devono restare chiuse e con strumenti di controllo atti ad impedire accessi abusivi. Il personale in servizio presso l'Azienda ha accesso ai locali esclusivamente per l'adempimento della prestazione lavorativa. Il personale che espleta servizi strumentali (es.: pulizia dei locali) o si occupa della manutenzione e dei servizi accessori, deve essere espressamente autorizzato ad accedere alle aree di sicurezza. L'assegnazione degli spazi di lavoro deve avvenire secondo criteri tali da impedire la promiscuità di permanenza e di utilizzazione tra:

- personale incaricato del trattamento di dati personali;

- personale non incaricato di trattamento di dati personali;

- soggetti estranei all'Azienda

Il personale dipendente incaricato del trattamento ha accesso ai dati esclusivamente sulla base delle esigenze di servizio, conformemente ai seguenti principi:

- la necessità di trattamento;

- il minimo livello di conoscenza dei dati.

I Responsabili del trattamento devono vigilare affinché venga disciplinato e controllato l'accesso, il transito e la permanenza di persone estranee all'attività lavorativa nelle aree e nei locali adibiti a luoghi di lavoro, con particolare attenzione agli spazi in cui vengono custodite banche di dati o ove vengono trattati dati sensibili o giudiziari. È altresì compito del Responsabile vigilare sull'introduzione in tali aree di oggetti, apparecchiature, sostanze o materiali che possono favorire il sorgere di rischi. Devono essere previsti procedure, accorgimenti e strumenti per:

- consentire l'accesso alle aree dove vengono custoditi e trattati i dati al solo personale autorizzato, ivi compresi i locali destinati al personale addetto alla video sorveglianza;

- ostacolare l'accesso abusivo ai dati;

- segnalare la presenza di intrusi.

2. ARCHIVI CARTACEI TEMPORANEI

La gestione degli archivi cartacei temporanei si ascrive alla competenza del Responsabile del trattamento. Lo stesso individua le tipologie dei documenti contenenti i dati sensibili e giudiziari ed i dipendenti incaricati dei relativi trattamenti. Il Responsabile dovrà assicurare che la documentazione venga custodita in armadi dotati di serratura, le cui chiavi dovranno essere conservate in modo appropriato. I documenti contenenti dati sensibili o giudiziari devono essere conservati secondo modalità che precludano la visione, in occasione della consultazione di documenti di altro genere, mediante creazione di sottofascicoli in busta chiusa, con sottoscrizione dello stesso Responsabile o di un incaricato. Il Responsabile deve garantire l'integrità dei sottofascicoli in occasione dell'accesso all'archivio da parte di soggetti non legittimati alla consultazione dei dati sensibili o giudiziari.

2.1. Archivi cartacei di deposito

L'archivio cartaceo di deposito deve essere controllato in considerazione della circostanza che l'accesso a siffatta documentazione non è pubblico. La consultazione potrà avvenire esclusivamente da parte del personale autorizzato o da parte di estranei autorizzati dal Responsabile. Il Responsabile dell'archivio cartaceo deve annotare su apposito registro gli estremi di ogni consultazione, precisando la data, la struttura richiedente, l'identità del soggetto che procede alla consultazione, l'oggetto della consultazione, le operazioni effettuate. I documenti contenenti dati sensibili o giudiziari devono essere conservati secondo modalità che precludano la visione, in occasione della consultazione di documenti di altro genere, mediante creazione di sottofascicoli in busta chiusa, con sottoscrizione dello stesso Responsabile o di un incaricato. Il Responsabile deve garantire l'integrità dei sottofascicoli in occasione dell'accesso da parte di soggetti non legittimati alla consultazione dei dati sensibili o giudiziari.

2.2. Selezione e scarto

La selezione e lo scarto della documentazione deve avvenire nel rispetto delle prescrizioni normative vigenti.

2.3. Altre misure per il rispetto dei diritti degli interessati

L'Azienda al fine di garantire il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale dovrà:

- predisporre appropriate distanze di cortesia, tenendo conto dell'eventuale uso di apparati vocali o di barriere;
- predisporre soluzioni tali da prevenire, durante colloqui, l'indebita conoscenza da parte di terzi di informazioni idonee a rilevare lo stato di salute;
- predisporre opportuni accorgimenti volti ad assicurare che, ove necessario, possa essere data correttamente notizia o conferma anche telefonica, ai soli terzi legittimati, di una prescrizione di pronto soccorso.

3. ISTRUZIONI PER IL TRATTAMENTO DEI DATI

Il Responsabile del trattamento dei dati è tenuto ad effettuare controlli sulle attività degli incaricati del trattamento, al fine di garantire la puntuale applicazione delle disposizioni contenute nel Codice. Ogni Responsabile informa annualmente gli incaricati dell'attivazione di sistemi di controlli legati a criteri in parte statistici in parte casuali. I responsabili, preferibilmente, precisano le istruzioni per il corretto trattamento dei dati, in forma scritta. E' sempre ammessa la diffusione di istruzioni in forma orale, in particolare allorquando vi sia l'urgenza di salvaguardare i principi in materia di trattamento dei dati personali. Deve in ogni caso garantirsi l'osservanza delle misure minime di sicurezza, contenute negli artt. 33 – 36 del d.lgs. n. 196 del 2003 e nel relativo allegato B, indifferentemente dalla natura del supporto contenente dati.

3.1. Trattamenti senza l'ausilio di strumenti elettronici

Il trattamento di dati senza strumenti elettronici, coinvolge i dati contenuti in tutti i supporti cartacei o simili che, comunque non richiedano l'uso di elaboratori elettronici. Ove esistano copie o riproduzioni di documenti che contengono dati personali, le medesime devono essere protette con le stesse misure di sicurezza applicate agli originali.

3.1.1. Custodia

- I documenti contenenti dati personali, devono essere custoditi in modo da non essere accessibili alle persone non incaricate del trattamento, mediante localizzazione presso spazi con accesso riservato (es. armadi o cassetti chiusi a chiave).
- I documenti contenenti dati personali prelevati dagli archivi per l'attività quotidiana, devono essere ivi collocati al termine della giornata.
- I documenti contenenti dati personali non devono rimanere incustoditi su scrivanie o tavoli di lavoro.

3.1.2. Comunicazione

La diffusione dei dati personali deve avvenire in base al principio dello "stretto indispensabile", talché non devono essere condivisi, comunicati o inviati a soggetti o istituzioni che non ne abbiano bisogno per lo svolgimento delle funzioni lavorative, a prescindere dall'eventuale qualifica di responsabili o incaricati di altra struttura. I dati non devono essere comunicati all'esterno della struttura, e comunque a soggetti terzi, se non previa autorizzazione.

3.1.3. Distruzione

Qualora sia necessario distruggere i documenti contenti dati personali, questi devono essere soppressi mediante apparecchi "distruggi documenti" o, in assenza, attraverso modalità che impediscano qualsiasi ricomposizione.

3.1.4. Istruzioni per il trattamento di dati sensibili e/o giudiziari

I documenti contenenti dati sensibili e/o giudiziari devono essere sottoposti al controllo dei responsabili i quali, a loro volta, potranno avvalersi degli incaricati per la custodia e/o il trattamento. Il Responsabile deve impedire l'accesso a persone prive di autorizzazione nei luoghi e nei momenti in cui si trattano dati sensibili e/o giudiziari.

Conseguentemente, il trattamento di dati sensibili e/o giudiziari contenuti in documenti cartacei deve avvenire per il tempo strettamente necessario al trattamento, con successiva immediata archiviazione dei dati.

L'archiviazione dei documenti cartacei contenenti dati sensibili e/o giudiziari deve avvenire in locali ad accesso controllato, utilizzando armadi o cassetti chiusi a chiave.

Per accedere agli archivi contenenti dati sensibili e/o giudiziari fuori orario di lavoro è necessario ottenere una preventiva autorizzazione da parte del Responsabile oppure procedere all'identificazione su un apposito registro.

3.2. Trattamenti con l'ausilio di mezzi elettronici

Per trattare i dati mediante dispositivi informatici, deve seguirsi una procedura di autenticazione che consenta l'identificazione del Responsabile o dell'Incaricato, mediante "credenziali di autenticazione". Le "credenziali di autenticazione" consistono in un user- ID, associato ad una parola chiave segreta password. Le user-ID e password individuali per l'accesso alle applicazioni non devono essere mai condivise con altri soggetti, anche se incaricati del trattamento. Nel caso in cui occorre permettere l'accesso da parte di altri utenti, è necessario richiedere la generazione di una nuova password. Per i PC collegati in rete, i Responsabili e gli Incaricati devono superare le procedure di identificazione, quali formalità preliminari per accedere alle risorse presenti nella rete aziendale; nel caso di utilizzo di applicazioni centralizzate, i responsabili e gli incaricati devono provvedere anche

alla propria identificazione sul sistema applicativo centrale, secondo le modalità e le regole previste dall'applicativo stesso. Tutti i Responsabili e gli Incaricati che utilizzano un personal computer per il trattamento di dati personali non collegato in rete, sono tenuti a proteggere l'accesso alla propria postazione di lavoro attivando una password (BIOS del PC e/o del sistema operativo).

3.2.1. Gestione delle password

La password è assegnata ai Responsabili ed agli Incaricati mediante sistemi meccanici che consentano l'enucleazione di password conformi alle prescrizioni contenute nell'Allegato B del d.lgs. n. 196 del 2003 (almeno 8 caratteri) e la periodica disattivazione/sostituzione. I Responsabili devono garantire l'esclusività dell'uso della password, in particolare impedendo che incaricati, o altri, si avvalgano di credenziali di autenticazione a qualunque titolo percepite. Nessuno deve annotare la propria password su supporti facilmente rintracciabili e, soprattutto, in prossimità della postazione di lavoro utilizzata. I Responsabili devono altresì accertarsi che gli incaricati cambino la password almeno ogni sei mesi, ovvero se trattano dati sensibili e/o giudiziari ogni tre mesi.

3.2.2. Custode delle password

In caso di assenza od impedimento dell'incaricato e contestuale esigenza di accedere ai dati detenuti presso banche dati o p.c. in uso all'incaricato, i responsabili devono attivare procedure di accesso temporaneo, mediante generazione di nuove credenziale di autenticazione. Le nuove credenziali di autenticazioni devono essere disattivate al termine della sessione straordinaria di lavoro. Conformemente a quanto previsto nel punto 10 dell'all. "B - Disciplinare tecnico" del Codice, il responsabile deve accertarsi che sia fornita adeguata comunicazione all'incaricato del sopravvenuto accesso al p.c. o alla banca dati da parte di altro incaricato.

3.2.3. Presenza di estranei all'azienda

I Responsabili devono garantire che le attività degli incaricati non vengano espletate alla presenza o secondo modalità che consentano ad estranei, di acquisire dati e/o informazioni detenute dall'azienda. A tal fine i Responsabili devono impartire istruzioni finalizzate ad evitare che personale estraneo o visitatori restino negli spazi ove si trattano dati personali. In ogni caso, gli incaricati sono tenuti a riporre i documenti contenenti dati personali secondo modalità che ne impediscano al visione a qualunque soggetto non legittimato i visitatori. In caso di allontanamento dal p.c. l'incaricato deve attivare la procedura c.d. "salvaschermo", al fine di evitare la visione dei documenti in lavorazione.

3.2.4. Istruzioni per il trattamento di dati sensibili e/o giudiziari

I dati anagrafici devono essere conservati separatamente da quelli sanitari che, invece, se contenuti in elenchi, registri o banche dati devono essere trattati con "tecniche di cifratura o codici identificativi che consentano di identificare gli interessati solo in caso di necessità".

3.2.5. Distruzione dei dati

I supporti magnetici od ottici contenenti dati personali devono essere cancellati prima di essere riutilizzati. Se ciò non è possibile, essi devono essere distrutti secondo modalità che ne impediscano la ricomposizione.

3.3. Istruzioni per la regolarizzazione dei rapporti con i fornitori: Informativa

Ogni struttura Aziendale dovrà regolarizzare i rapporti con ogni fornitore dell'Azienda mediante l'invio dell'informativa prevista dall'art. 13 del D.Lgs 196/03, tramite raccomandata A/R o fax. La ricevuta dell'avvenuto invio deve essere conservata presso la struttura.

3.3.1. Designazione dei Responsabili esterni del trattamento

I Responsabili del trattamento individuati, dovranno farsi carico di designare i soggetti esterni che trattano dati per conto della propria struttura in virtù di un contratto in essere, a Responsabili esterni del trattamento utilizzando lo schema previsto per quanto concerne i contratti di Assistenza/Manutenzione dei sistemi hardware e software e per i servizi esternalizzati che prevedono il trattamento di dati comuni/sensibili/giudiziari (es. gestione cartelle cliniche, diagnostica in convenzione ecc.).

3.4. Istruzioni per regolarizzare il trattamento dei dati dei dipendenti/collaboratori

La UOC Gestione delle Risorse Umane dovrà farsi carico di informare il dipendente/collaboratore mediante opportuna procedura dell'informativa prevista dall'art. 13 del D.Lgs 196/03. L'informativa dovrà essere allegata al contratto di assunzione, di collaborazione, di consulenza ecc. di nuova adozione.