AOU AL Azienda Ospedaliero Universitaria di ALESSANDRIA Santi Antonio e Biagio e Cesare Arrigo

Via Venezia, 16 – 15121 ALESSANDRIA
Tel . 0131 206111 – www.ospedale.al.it
info@ospedale.al.it
asoalessandria@pec.ospedale.al.it (solo certificata)
C.F. – P.I. 01640560064

VADEMECUM PRIVACY AL PERSONALE – REGOLAMENTO EUROPEO 679/2016

Il diritto alla riservatezza deve essere garantito in particolar modo per i cittadini che entrano in contatto con le strutture sanitarie, e quindi per i dati relativi alla salute a loro afferenti.

I dati relativi alla salute sono quelli "attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute" (art. 4 del Regolamento Europeo). Sono ricompresi nella più vasta categoria dei dati soggetti a trattamento speciale (art. 9 Regolamento europeo), in quanto in grado di rivelare dettagli molto intimi della persona, e per questo vi è una tutela rafforzata, di tali dati.

L'Azienda Ospedaliero- Universitaria effettua tanti trattamenti di dati, oltre a quelli sanitari e tutti devono avvenire nel rispetto dei principi stabiliti dal Regolamento UE 679/2016:
- in modo lecito, corretto e trasparente nei confronti dell'interessato;
- raccolti per finalità determinate esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
-esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;
-trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o da danni accidentali.

Con riferimento a tali principi si forniscono le seguenti istruzioni operative minime.

1. Istruzioni in tema di sicurezza:

· il personale autorizzato, per tutto il periodo in cui effettua le operazioni di trattamento dei dati, non deve mai perdere di vista i documenti, adempiendo ad un preciso obbligo di custodia dei medesimi;
· il personale autorizzato deve controllare che i documenti siano sempre completi ed integri;
· in caso di abbandono, anche temporaneo, dell'ufficio, il personale autorizzato non deve mai lasciare incustoditi i documenti (sulla scrivania, su tavolini di reparto, sui carrelli); è infatti necessario identificare un luogo sicuro di custodia che dia sufficienti garanzie di protezione da accessi non autorizzati (un armadio o un cassetto chiusi a chiave, una cassaforte, una stanza chiusa a chiave, ecc.); ove si utilizzi un contenitore chiuso a chiave occorre accertarsi che non esistano duplicati abusivi delle chiavi e che le stesse siano in possesso solo del personale autorizzato;
· occorre in particolare accertarsi che nessun visitatore o terzo estraneo (addetto alla manutenzione, alle pulizie, un collega non autorizzato, fornitori, informatori scientifici) possa venire a conoscenza (anche per cause accidentali) del contenuto dei documenti;

· al momento della consegna di copie dei documenti ai destinatari è necessario adottare tutte le garanzie di sicurezza, quali l'utilizzo di buste sigillate;
· la parola chiave di accesso alla postazione informatica deve essere custodita con la massima attenzione e segretezza e non deve essere divulgata o comunicata a terzi;
· la parola chiave non deve contenere riferimenti facilmente riconducibili al personale autorizzato;
· il personale autorizzato è responsabile di ogni utilizzo indebito o non consentito della parola chiave di cui sia titolare;
· in caso di assenza, anche momentanea, dalla propria postazione di lavoro, devono essere adottate misure atte ad escludere che soggetti non autorizzati possano acquisire la conoscenza di informazioni o accedere alle banche dati;
. coloro che sono autorizzati a detenere e utilizzare la casella di posta elettronica aziendale sul proprio smartphone, custodiscono lo stesso con estrema diligenza prevenendo qualsiasi utilizzo indebito dello stesso;
·occorre fare particolare attenzione alla spedizione, a mezzo di posta elettronica, di file o di messaggi contenenti categorie particolari di dati personali quali i dati relativi alla salute. 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 perla 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.

2. Istruzioni per l'utilizzo degli strumenti di lavoro

2.1 Utilizzo del telefono e del fax:

· nel caso in cui sia necessario effettuare comunicazioni telefoniche agli interessati, occorre aver chiesto preliminarmente all'interessato medesimo l'autorizzazione a conferire con chiunque risponda all'apparecchio. In caso di risposta negativa è necessario chiedere in alternativa un numero differente e riservato;
· occorre fare attenzione a discutere, comunicare o comunque trattare dati personali e o appartenenti a categorie particolari per telefono in presenza di terzi non autorizzati che potrebbero inavvertitamente venire a conoscenza di tali dati;
· in caso di invio di documentazione a mezzo fax, bisogna prestare attenzione alla corretta digitazione del numero cui inviare il documento e verificarne l'esattezza, nonché attendere la stampa del rapporto di trasmissione;
· qualora vengano trasmessi dati relativi alla salute, è opportuno anticipare l'invio del fax avvertendo il destinatario, assicurarsi che il ricevimento avvenga nelle mani del medesimo ed evitare che soggetti estranei o non autorizzati possano conoscere il contenuto della documentazione inviata;
- non lasciare incustoditi presso il fax documentazione contenente dati personali con particolare attenzione per quelli contenenti dati particolari;
- nel caso di ricevimento via fax di comunicazione contenente dati personali particolari provvedere all'immediato ritiro della stessa;
· l'apparecchio fax deve essere sempre collocato in luogo non accessibile a terzi non autorizzati.

2.2 Utilizzo della fotocopiatrice e della stampante:

- nell'esecuzione delle operazioni di fotocopiatura o di stampa la documentazione non deve essere accessibile a chi non è autorizzato al trattamento;
· in caso di stampa o duplicazione non riuscite di documentazione contenente dati personali e o appartenenti a categorie particolari, occorre evitare di gettare i fogli nel cestino senza aver provveduto a rendere illeggibile il contenuto dei dati (mediante apposita macchinetta tritatutto o distruzione manuale in piccoli pezzi);
· è pericoloso utilizzare le fotocopie o le stampe di documentazione contenente dati personali non riuscite come carta per appunti;
· occorre utilizzare con attenzione le macchine fotocopiatrici di ultima generazione che possono scannerizzare e memorizzare il documento, talvolta conservando il file elettronico dello stesso;

2.3 Utilizzo di supporti di memorizzazione:

· i supporti rimovibili, come ad esempio unità USB o cd rom, che contengano categorie particolari di dati o dati giudiziari possono essere riutilizzati solo se i dati precedentemente memorizzati non siano più visionabili da parte di terzi che procedano al riutilizzo del supporto medesimo. Tali dispositivi qualora contengano dati personali, devono essere conservati in contenitori muniti di serratura.

2.4 Utilizzo di software

- è vietato installare e usare qualunque software, anche se scaricato da internet, senza la previa autorizzazione da parte di soggetto titolato. 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.

3. 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;
. se deve essere chiamato un paziente in una sala d'attesa o in un corridoio si deve prestare la massima attenzione al tono della voce per evitare di essere uditi da una pluralità di altri pazienti in attesa o in transito. E' preferibile piuttosto chiamare il paziente con l'iniziale del nome e cognome
· obbligo di riservatezza e segretezza: il personale autorizzato al trattamento deve mantenere l'assoluta segretezza sulle informazioni di cui venga a conoscenza nel corso delle operazioni di trattamento. La diffusione di dati relativi alla salute è tassativamente vietata;
· controllo dell'identità del richiedente: nel caso di richieste di comunicazioni di dati (presentate per telefono o via fax) occorre verificare l'identità del soggetto richiedente, ad esempio formulando una serie di quesiti (accertamento sommario);
· identificazione dell'interessato e controllo dell'esattezza dei dati: in alcuni casi è necessaria l'identificazione del soggetto interessato per esigenze di garanzia di correttezza del trattamento (soprattutto per quanto riguarda la raccolta di dati anagrafici di cittadini stranieri), facendo attenzione alla digitazione ed all'inserimento corretto dei dati identificativi dell'interessato medesimo;

4. Cautele da seguire per la corretta comunicazione dei dati:

· la richiesta di comunicazione di dati personali e/o di categorie particolare di dati può essere evasa nei confronti dell'interessato o di un terzo a ciò delegato (per iscritto) o legittimato;
· la comunicazione di dati relativi alla salute deve essere sempre effettuata da un medico o da personale sanitario a ciò delegato;
· 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;
- i flussi documentali all'interno dell'ente, qualora la documentazione contenga dati relativi alla salute, devono avvenire nel rispetto della riservatezza degli interessati, adottando misure che siano idonee a limitare la conoscenza dei dati medesimi da parte dei soli soggetti destinatari;
- la spedizione di documenti contenenti categorie particolari di dati o dati giudiziari deve avvenire in busta chiusa. In alcuni casi, può essere utile utilizzare una busta non intestata, al fine di garantire la riservatezza del destinatario,
- i giustificativi recanti attestazione delle prestazioni sanitarie svolte che vengono richiesti dai lavoratori per avere titolo a permessi dal datore di lavoro devono essere emessi senza l'intestazione del reparto e firmati dal personale amministrativo.

5. Istruzioni concernenti operazioni di trattamento:

raccolta: prima di procedere alla raccolta dei dati personali, deve essere fornita l'informativa all'interessato o in caso di minore o incapace di intendere e volere al rappresentante legale, occorre inoltre procedere alla raccolta dei dati con la massima cura verificando l'esattezza degli stessi;
conservazione: i documenti o gli atti che contengono categorie particolari di dati o dati 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;

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

cancellazione: i dati personali devono essere cancellati se non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati, ovvero conservati in una forma che non consenta l'identificazione dell'interessato