Informatica e telecomunicazioni
Responsabile Antonio Fumagalli

ISTRUZIONI OPERATIVE PRIVACY PER L'INCARICATO DEL TRATTAMENTO DEI DATI

Il titolare del trattamento dati, conformemente a quanto stabilito dall'art. 30 del decreto legislativo n. 196/2003 (codice in materia di protezione dei dati personali) e dal paragrafo 28 del disciplinare tecnico (allegato B al codice), con il presente atto impartisce agli incaricati del trattamento le istruzioni privacy da rispettare nello svolgimento delle operazioni di trattamento dati e per l'intero ciclo necessario allo svolgimento delle stesse.

1. Istruzioni per la protezione del documento cartaceo

1.1. documenti oggetto di trattamento possono essere affidati soltanto a soggetti appositamente autorizzati e nel rispetto del proprio ambito di trattamento;

1.2. durante il trattamento, i documenti devono essere custoditi e controllati in modo che ad essi non accedano persone prive di autorizzazione;

1.3. concluso il trattamento, i documenti devono essere collocati in una stanza presidiata dal personale autorizzato oppure in un locale/armadio chiudibile;

1.4. in occasione della trasmissione dei documenti che avviene all'interno dell'ospedale, devono essere adottati tutti gli accorgimenti necessari e idonei onde evitare che le informazioni riservate possano essere lette sia pure accidentalmente da chi non è autorizzato (ad esempio trasporto mediante cartelle chiuse);

1.5. in occasione della trasmissione dei documenti al paziente, gli stessi devono essere risposti in busta chiusa, priva all'esterno di informazioni sensibili, da consegnarsi direttamente all'interessato o al terzo delegato per iscritto;

1.6. i documenti recanti dati genetici possono essere trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati ed ai soggetti specificatamente autorizzati ad accedervi;

1.7. i documenti recanti dati genetici possono essere trasportati all'esterno dei locali riservati al loro trattamento soltanto mediante contenitori muniti di serratura o altri dispositivi equipollenti;

1.8. i documenti su cui sono riportati dati personali non devono essere riciclati (ad esempio per carta da minuta o per le fotocopie) onde evitare il rischio che gli stessi possano essere letti da chi non è autorizzato;

1.9. i documenti possono essere affissi in stanze ad accesso selezionato a condizione che siano posizionati in modo tale da evitare che le informazioni possano essere lette sia pure

Informatica e telecomunicazioni
Responsabile Antonio Fumagalli

accidentalmente da chi non è autorizzato (ad esempio sul retro della porta, sulla parte interna dell'anta di una armadio, in un cassetto, eccetera).

2. Istruzioni per la protezione della persona (se pertinente)

2.1 in sala d'attesa devono essere adottate modalità di chiamata del paziente che prescindono dalla sua individuazione nominativa (contatto diretto, numero, tabellone elettronico);

2.2 in sala d'attesa deve essere istituita la distanza di cortesia tra utente allo sportello e utente in fila e, se ciò non è realizzabile per le dimensioni della stanza, deve essere adottato un comportamento improntato alla massima prudenza onde evitare l'indebita conoscenza da parte di terzi di informazioni idonee a rivelare lo stato di salute del paziente;

2.3 i colloqui sanitari devono svolgersi in locali protetti e, qualora ciò non sia possibile, deve essere adottato un comportamento improntato alla massima prudenza onde evitare l'indebita conoscenza da parte di terzi di informazioni idonee a rivelare lo stato di salute del paziente;

2.4 la prestazione sanitaria, compresa l'eventuale documentazione di anamnesi, deve avvenire in assenza di situazioni di promiscuità derivanti dalle modalità o dai locali prescelti;

2.5 la prestazione deve essere erogata nel rispetto della dignità del paziente, soprattutto in riferimento a fasce deboli (minori, disabili, anziani) o situazioni particolari (interruzione della gravidanza, malato di hiv/aids) che richiedono particolare sensibilità;

2.6 devono essere rispettate le indicazioni del paziente circa i soggetti autorizzati a ricevere comunicazioni sullo stato di salute e i soggetti autorizzati a recare visita in occasione del ricovero;

2.7 deve essere prevenuto il rischio che gli estranei possano collegare il paziente al suo stato di salute: ad esempio non utilizzare buste con l'indicazione del reparto di provenienza per la spedizione del referto presso l'abitazione del paziente.

3. Istruzioni per la protezione della credenziale di autenticazione ai programmi informatici (PIN –Personal Identification Number - della smart card)

3.1 L'Azienda Ospedaliera ha deciso di dotarsi di un sistema di autenticazione alle risorse informatiche mediante utilizzo della smart card (SISS-operatore o aziendale). Tale sistema prevede la gestione automatica delle password dei programmi ai quali si accede, in modo che l'operatore non debba conoscere null'altro che il PIN associato alla propria smart card;

Informatica e telecomunicazioni
Responsabile Antonio Fumagalli

3.2 Il PIN della smart card è personale, segreto, non cedibile e deve essere custodito in modo diligente mediante l'adozione delle necessarie e idonee cautele;

3.3 Il PIN della smart card è composto da otto caratteri. Nel caso in cui l'accesso al programma non venga effettuato mediante smart card la password deve essere composta da almeno otto caratteri o, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito. La password deve rispettare gli stessi criteri di robustezza previsti per il PIN della smart card e deve essere modificata ogni 3 mesi;

3.4 Nel PIN della smart card non devono essere immessi riferimenti agevolmente riconducibili alla propria persona (ad esempio nome, cognome, data di nascita, nome del coniuge);

3.5 Il PIN della smart card deve essere modificato al primo utilizzo (ossia successivamente alla consegna della busta chiusa contenente l'informativa sull'utilizzo e la busta cieca contenente codici PIN e PUK);

3.6 Il PIN della smart card non deve essere trascritto su promemoria in vista (ad esempio post-it sul PC o sulla smart card stessa);

Durante una sessione di trattamento, lo strumento elettronico non deve essere lasciato incustodito e

ASST Papa Giovanni XXIII - Piazza OMS, 1 - 24127 Bergamo - Tel. 035.267111 - www.asst-pg23.it
Informatica e telecomunicazioni - Tel. 035.2675089 - Fax 035.2674845 - sistinformativo@asst-pg23.it