ALLEGATO N. 3

1. Descrizione della CERTIFICAZIONE DI CONFORMITA'

Si elencano qui di seguito tutti i punti dell'allegato B) del D.Lgs 196/2003 e del DPS aziendale sui quali si richiede una certificazione di conformità da parte dell'impresa:

1. **Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.**

   Si richiede che nell'ambito della Vostra fornitura i trattamenti siano consentiti agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

2. **Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometria dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.**

   Si richiede che nell'ambito della vostra fornitura le credenziali di autenticazione consistano in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata.

5. **La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.**

   Si richiede che nell'ambito della Vostra fornitura i sistemi prevedano l'utilizzo di parola chiave composte da almeno otto caratteri. Tale parola chiave deve poter essere modificabile autonomamente dall'incaricato al trattamento, senza che questa modifica implichi un supporto sistemistico o un intervento di terzi. Inoltre si richiede che il sistema obblighi l'incaricato a cambiare la propria parola chiave trimestralmente, impedendo, in caso di mancata modifica, l'accesso ai dati.

6. **Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.**

   Si richiede che nell'ambito della Vostra fornitura i sistemi prevedano che il codice per l'identificazione, non possa essere assegnato ad altri incaricati.

7. **Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.**

OSPEDALE NIGUARDA CA' GRANDA MILANO AZIENDA - OSPEDALIERA

Si richiede che nell'ambito della Vostra fornitura i sistemi prevedano che le credenziali di autenticazione non utilizzate da almeno sei mesi siano automaticamente disattivate dal sistema stesso,senza interventi esterni di disattivazione.

12. **Quando per gli incaricati sono individuati profili di autorizzare di ambito diverso è utilizzato un sistema di autorizzazione.**

    Si richiede che nell'ambito della Vostra fornitura sia previsto un sistema di autorizzazione degli accessi.

16. **I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.**

    Si richiede che nell'ambito della Vostra fornitura i dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici che siano aggiornati con cadenza almeno semestrale.

17. **Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.**

    Si richiede che nell'ambito della Vostra fornitura sia previsto un aggiornamento almeno semestrale dei programmi volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti.

22. **I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.**

    Si richiede che nell'ambito della Vostra fornitura sia esplicitamente escluso l'uso di supporti rimovibili quali locazioni standard di dati sensibili. Tali supporti rimovibili non devono essere riutilizzati neanche per esigenze di backup.

23. **Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non seriori a sette giorni.**

    Si richiede che nell'ambito della Vostra fornitura sia esplicitamente previsto un piano di recovery dei dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.

24. **Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'art. 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali**

OSPEDALE NIGUARDA CA' GRANDA MILANO AZIENDA - OSPEDALIERA

riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.

Si richiede che nell'ambito della Vostra fornitura sia esplicitamente previsto che i dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, siano disgiunti dagli altri dati personali che permettono di identificare direttamente gli interessati.

25. **Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve, dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.**

Si richiede che nell'ambito della Vostra fornitura tutti gli interventi effettuati siano certificati come conformi all'allegato B) del D.lg. 196/2003.

Dal DPS Aziendale. Tutti i collegamenti locali con modem non sono ritenuti conformi.

Si richiede che nell'ambito della Vostra fornitura non siano previsti modem per nessun motivo. In caso di necessità di manutenzione remota, la S.C. Gestione, ricerca e sviluppi informatici - ICT mette a Vostra disposizione delle modalità d'accesso via RAS e VPN. Si prega l'impresa in oggetto di contattare ICT per esigenze di accesso remoto. Tutte gli altri collegamenti per accesso remoto non in gestione alla S.C. Gestione, ricerca e sviluppi informatici – ICT non sono ritenuti conformi.

2. Descrizione dell'ELENCO DEGLI INCARICATI al trattamento

In base a quanto previsto ai punti 1,2,3,4 dell'allegato B) del D.lg. 196/2003 è indispensabile procedere alla nomina di incaricati di tutti quei soggetti che hanno accesso ai dati personali o sensibili a fini manutentivi o, più in generale, per erogare il servizio oggetto di fornitura – o che in ogni caso trattano dati personali. Si richiede quindi che al più presto vengano comunicate alla S.C. Gestione, ricerca e sviluppi informatici – ICT gli estremi identificativi del personale coinvolto nel trattamento al fine di completare gli elenchi degli incaricati.

Al fine di procedere alla nomina dell'incaricato sono indispensabili le seguenti informazioni:

- ✓ Nome e cognome
- ✓ Data e luogo di nascita
- ✓ Impresa di appartenenza
- ✓ Compiti specifici che il soggetto dovrà svolgere presso le nostre sedi.

Nel caso la persona cessi di svolgere le funzioni per le quali ha ricevuto l'incarico, anche solo per un periodo superiore a sei mesi, dovrà esserne data tempestiva comunicazione alla S.C. Gestione, ricerca e sviluppi informatici – ICT che provvederà a revocare i diritti di accesso ai locali e ai sistemi, e se del caso l'incarico al trattamento.

OSPEDALE NIGUARDA CA' GRANDA MILANO AZIENDA - OSPEDALIERA

ALLEGATO N. 3

CERTIFICAZIONE DI CONFORMITA'

OGGETTO: attestazione di conformità del sistema informatico al D.Lgs 196/2003 "codice in materia di protezione dei dati personali"

Il/La sottoscritto/a_____ in funzione di

rappresentante legale dell'impresa _____ con la presente

dichiara che tutte le forniture e relative gestioni (già in essere o future) presso la A.O. Ospedale Niguarda Ca' Granda sono conformi a quanto previsto nella "certificazione di conformità" richiesta dalla Vostra Azienda.

Data_____

Timbro e firma

OSPEDALE NIGUARDA CA' GRANDA MILANO AZIENDA - OSPEDALIERA