Azienda Socio-Sanitaria Territoriale (ASST) di Pavia
Sede Legale: Viale Repubblica, 34 - 27100 PAVIA
Codice Fiscale/Partita I.V.A. n. 02613080189
sito internet: www.asst-pavia.it

Allegato 3 – Sicurezza informatica.

Trattamento di dati personali e rispetto della normativa in tema di protezione di dati personali

L'Aggiudicatario verrà nominato da parte di ASST Pavia Responsabile del trattamento ai sensi dell'art. 28 del Regolamento UE n. 2016/679 sulla protezione delle persone fisiche, con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (nel seguito anche "Regolamento UE"), per tutta la durata del contratto. A tal fine il Responsabile sarà autorizzato a trattare i dati personali necessari per l'esecuzione delle attività oggetto del contratto e si impegna ad effettuare, per conto del Titolare, le sole operazioni di trattamento necessarie per fornire il servizio oggetto del presente contratto, nei limiti delle finalità ivi specificate, nel rispetto del Codice Privacy, del Regolamento UE (nel seguito anche "Normativa in tema di trattamento dei dati personali") e delle istruzioni nel seguito fornite.
L'Aggiudicatario si dovrà impegna a presentare, su richiesta dell'Amministrazione, garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse per l'adozione di misure tecniche ed organizzative adeguate volte ad assicurare che il trattamento sia conforme alle prescrizioni della normativa in tema di trattamento dei dati personali.

Nell'esercizio delle proprie funzioni, il Responsabile si dovrà impegnare a:

a) rispettare la normativa vigente in materia di trattamento dei dati personali, ivi comprese le norme che saranno emanate nel corso della durata del contratto;
b) trattare i dati personali per le sole finalità specificate e nei limiti dell'esecuzione delle prestazioni contrattuali;
c) trattare i dati conformemente alle istruzioni impartite dal Titolare e di seguito indicate che il Fornitore si impegna a far osservare anche alle persone da questi autorizzate ad effettuare il trattamento dei dati personali oggetto del presente contratto, d'ora in poi "persone autorizzate"; nel caso in cui ritenga che un'istruzione costituisca una violazione del Regolamento UE sulla protezione dei dati o delle altre disposizioni di legge relative alla protezione dei dati personali, il Fornitore deve informare immediatamente il Titolare del trattamento;
d) garantire la riservatezza dei dati personali trattati nell'ambito del presente contratto e verificare che le persone autorizzate a trattare i dati personali in virtù del presente contratto:
    - si impegnino a rispettare la riservatezza o siano sottoposti ad un obbligo legale appropriato di segretezza;
    - ricevano la formazione necessaria in materia di protezione dei dati personali;
    - trattino i dati personali osservando le istruzioni impartite dal Titolare per il trattamento dei dati personali al Responsabile del trattamento;
e) adottare politiche interne e attuare misure che soddisfino i principi della protezione dei dati personali fin dalla progettazione di tali misure (privacy by design), nonché adottare misure tecniche ed organizzative adeguate per garantire che i dati personali siano trattati, in

ossequio al principio di necessità ovvero che siano trattati solamente per le finalità previste e per il periodo strettamente necessario al raggiungimento delle stesse (privacy by default);

f) valutare i rischi inerenti il trattamento dei dati personali e adottare tutte le misure tecniche ed organizzative che soddisfino i requisiti del Regolamento UE anche al fine di assicurare un adeguato livello di sicurezza dei trattamenti, in modo tale da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, modifica, divulgazione non autorizzata, nonché di accesso non autorizzato, anche accidentale o illegale, o di trattamento non consentito o non conforme alle finalità della raccolta;

Il fornitore deve tempestivamente fornire alla ASST ogni informazione o evidenza richiesta dallo stesso che sia in suo possesso o sotto il suo controllo, al fine di garantire la conformità della ASST alla legislazione vigente. L'applicazione della presente clausola deve avvenire senza alcun costo aggiuntivo e/o onere alcuno a carico della ASST.

Nel trattamento di dati personali dell'Ente realizzato in ottemperanza del presente accordo, il fornitore dovrà:

- implementare tutte le misure di sicurezza in conformità al Codice Privacy ed all'Allegato B al Codice Privacy (Disciplinare Tecnico in materia di misure minime di sicurezza);
- su ragionevole richiesta dell'Ente, riferire allo stesso sulle misure di sicurezza adottate.
- informare tempestivamente l'Ente di qualsiasi circostanza rilevante in relazione al trattamento dati dell'Ente realizzato in esecuzione dell'accordo.

Il Responsabile del trattamento deve mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al Regolamento UE, oltre a contribuire e consentire al Titolare - anche tramite soggetti terzi dal medesimo autorizzati, dandogli piena collaborazione - verifiche periodiche o circa l'adeguatezza e l'efficacia delle misure di sicurezza adottate ed il pieno e scrupoloso rispetto delle norme in materia di trattamento dei dati personali. A tal fine, il Titolare informa preventivamente il Responsabile del trattamento con un preavviso minimo di tre giorni lavorativi, fatta comunque salva la possibilità di effettuare controlli a campione senza preavviso. Nel caso in cui all'esito di tali verifiche periodiche, ispezioni e audit le misure di sicurezza dovessero risultare inadeguate rispetto al rischio del trattamento o, comunque, inidonee ad assicurare l'applicazione del Regolamento, l'Amministrazione diffiderà il Fornitore ad adottare tutte le misure più opportune entro un termine congruo che sarà all'occorrenza fissato. In caso di mancato adeguamento a seguito della diffida, resa anche ai sensi dell'art. 1454 cc, l'Amministrazione potrà risolvere il contratto ed escutere la garanzia definitiva, salvo il risarcimento del maggior danno.

Clausola di manleva
Il Fornitore solleva la ASST da ogni responsabilità e risponde degli eventuali inadempimenti o violazioni di legge perpetrate da suoi collaboratori/ausiliari o terzi, per ragioni imputabili in relazione alla perdita, furto o diffusione non autorizzata di dati.

Compatibilità
Tutte le applicazioni che prevedono la produzione di documenti di tipo sanitario devono prevedere l'integrazione e la piena compatibilità con il sistema CRS-SISS esistente in Lombardia.
Tale integrazione deve prevedere, previa validazione con l'ASST, almeno le seguenti funzioni minimali:

- La gestione della Firma Digitale tramite Carta Operatore;
- L'utilizzo dell'Anagrafica Pazienti Aziendale verso la quale deve essere disponibile piena e completa integrazione;
- L'invio dei documenti prodotti al Repository;
- L'utilizzo dei nomenclatori SISS;
- L'integrazione applicativa tramite middleware in uso presso l'ASST;
- L'eventuale notifica dei referti ai Domini Centrali del SISS.

L'integrazione deve avvenire sulla base delle specifiche previste dalle Linee Guida attive in Regione Lombardia recuperabili dal sito di progetto SISS http://www.siss.regione.lombardia.it/.

Con le stesse modalità devono essere sviluppate tutte le applicazioni che prevedono la Firma Digitale dei documenti prodotti: le modalità di firma, le regole di apposizione e di conservazioni devono essere le medesime previste al caso precedente anche quando non sia prevista la notifica al SISS del Documento Clinico Elettronico (DCE).

Modifiche al servizio
Tutte le modifiche riguardanti applicazioni, architettura, procedure operative, procedure di sicurezza e la relativa valutazione del rischio, devono essere notificate con sufficiente anticipo all'ASST per permetterne la tempestiva approvazione o il rifiuto delle stesse.

Governance
Il fornitore deve essere conforme ai requisiti di IT Governance dell'ASST, ed in particolare dovrà fornire informazioni su:

- schema aggiornato dell'infrastruttura/architettura IT che sarà oggetto di approvazione scritta da parte dell'ASST;
- schema dell'organizzazione IT (compresi i canali di comunicazione verso di essa), che ha in carico i servizi/soluzioni IT;
- modifiche riguardanti l'architettura e le procedure di sicurezza, nonché la valutazione del rischio a esse corrispondente.

Attività di sicurezza
E' responsabilità del fornitore:

- predisporre un piano delle sicurezza comprendete la periodicità dei vulnerabilty assesment, i piani di remediation, l'aggiornamento costante dei software, l'installazione di security patch, l'adozione di sistemi di ATP (Advanced Threat Protection);
- garantire la crittografia dei dati;
- garantire il controllo degli accessi al data center;
- fornire un documento di architettura di rete che dettagli dove sono localizzati i dati applicativi, le applicazioni che utilizzano tali dati, e la loro sicurezza. Ogni variazione o aggiornamento del documento di architettura, in particolare ogni cambiamento nel modello di scambio dei dati tra il fornitore e l'ASST e ogni cambiamento significativo delle

configurazioni di sicurezza devono essere comunicati e approvati da parte dell'ASST. La rete che ospita l'applicazione deve essere isolata da qualsiasi altra rete o cliente per il quale il fornitore lavori. L'ambiente applicativo dell'ASST dovrà utilizzare host e infrastrutture separati dagli altri clienti del fornitore.

- riferire costantemente alla ASST lo stato di applicazione ed evoluzione delle misure di sicurezza adottate;
- informare tempestivamente la ASST di qualsiasi circostanza rilevante in relazione al trattamento dati;
- riferire costantemente alla ASST lo stato di applicazione ed evoluzione delle misure di sicurezza adottate.

Manualistica

Il fornitore si impegna a consegnare copia cartacea ed elettronica di tutta la documentazione utente ed amministrativa del sistema oggetto di fornitura prima della messa in esercizio del sistema oggetto di fornitura, correttamente personalizzata per la propria installazione, comprensiva del dettaglio della configurazione adottata.

Il Fornitore deve garantire che durante lo svolgimento di tutte le attività collegate al servizio/soluzione IT erogato, la documentazione aziendale venga adeguatamente manutenuta, in conformità con le best practice e la normativa vigente, e che la documentazione aziendale sia protetta contro accesso, uso, perdita, alterazione o distruzione impropria.

Collaudi e Passaggio in produzione

Eventuali modifiche che impattano l'architettura e il servizio erogato devono essere portate a conoscenza dell'ASST, informandola circa la configurazione corrente, le modifiche proposte, le modalità e i risultati del test.
Il processo di autorizzazione alla messa in produzione deve essere conforme alle policy dell' ASST e soggetto a collaudi, che dovranno essere eseguiti prima di ogni cambiamento in produzione e che saranno sotto la responsabilità dell' ASST a prescindere dal supporto necessario da parte del fornitore per eseguire gli stessi. In particolare, sono da attuarsi i collaudi per le seguenti tipologie di fornitura:

- alla verifica e messa in funzione del sistema;
- al collaudo di tutte le apparecchiature oggetto della fornitura;
- alla piena e completa verifica funzionale in condizioni di esercizio simulando diversi cicli di funzionamento anche in condizioni di stress.

Il collaudo verificherà:

- la corrispondenza tra le caratteristiche funzionali e tecniche dichiarate e quelle riscontrate;
- l'avvenuta esecuzione delle sessioni di formazione per le diverse tipologie di utenti dell' ASST;
- l'interconnessione di tutte le componenti del sistema con la LAN aziendale e la piena raggiungibilità da essa;
- la correttezza di funzionamento di tutti i sottosistemi e del sistema nel suo complesso.

Tale collaudo avverrà sulla base di un piano di lavoro redatto dai referenti del Sistema Informativo e condiviso con il Capoprogetto del fornitore e dovrà essere adeguatamente documentato in ogni sua fase.

Accesso alle risorse della ASST

Solo gli utenti autorizzati dalla ASST per iscritto possono accedere alle informazioni e ai dati contenuti all'interno delle infrastrutture della ASST (di proprietà o concesse in uso) o infrastrutture di

terze parti utilizzate dalla ASST e situate in siti di soggetti terzi. Tutti gli accessi saranno concessi solo ai singoli individui. Account generici o condivisi sono assolutamente proibiti. Nessun dato o informazione contenuto all'interno dell'infrastruttura della ASST (di proprietà o concesse in uso) o in infrastrutture di terze parti utilizzate dalla ASST e situate in siti di soggetti terzi devono essere comunicati a terzi senza previa autorizzazione scritta da parte della ASST. Il fornitore deve comunicare tempestivamente alla ASST quando un suo dipendente autorizzato all'accesso lascia l'azienda temporaneamente o definitivamente, o non necessità più dell'accesso, o sono cambiati ruolo/privilegi nell'accedere ai beni della ASST.
Quando il contratto è risolto per qualsiasi ragione o è scaduto, tutti gli accessi devono essere immediatamente revocati. Il fornitore non sarà ulteriormente autorizzato ad accedere alle risorse della ASST.

Accesso fisico ai locali della ASST
La ASST comunicherà le regole di sicurezza e di accesso ai propri siti. Il fornitore deve consegnare alla ASST una lista con i nomi e i ruoli del suo personale o del personale dei subfornitori che possono avere accesso a siti della ASST. Il personale del fornitore oppure il personale dei subfornitori inclusi in tale elenco devono presentarsi alla reception della ASST, dove verrà consegnato un badge, che dovrà essere indossato in modo visibile e in ogni momento durante la visita presso i siti della ASST. Se una persona non è inclusa nella lista per qualsiasi ragione e ha bisogno di accedere al sito della ASST, verrà registrata presso la reception dopo aver mostrato un suo documento d'identità. Tale persona deve essere accompagnata in ogni momento dal personale della ASST. Se il personale del fornitore o il personale dei subfornitori, ha bisogno di accedere alle aree riservate (come le sale server, data center, gli armadi di rete, etc.), esso deve essere accompagnato in ogni momento dal personale della ASST.

Obbligo di riservatezza
Per tutta la durata del presente accordo e successivamente alla cessazione del medesimo per qualsiasi causa intervenuta, il fornitore si obbliga a:

- non utilizzare le Informazioni per scopi diversi, in tutto o in parte, da quelli contemplati dal contratto;

- mantenere riservati i fatti, documenti, progetti, dati e informazioni (intesi nella più ampia accezione dei termini) di cui verrà a conoscenza e/o disporrà in relazione al e/o in esecuzione del presente contratto (di seguito: Informazioni).

Eccezioni
Qualsiasi deroga alle disposizioni definite in queste clausole deve essere valutata ed eventualmente concessa dalla ASST in forma scritta.