ALLEGATO B AL CAPITOLATO TECNICO:

SOFTWARE GESTIONALE

(LOTTO 1 ID20SER027 CUC)

Consultazione preliminare di mercato

(Ex art. 66 Dlgs. n.50/2016)

Sommario

Specifiche non funzionali 3
Caratteristiche del sistema gestionale informatico 3
Contesto normativo 3
Requisiti generali 3
Data center e connettività 4
Accessibilità ed usabilità 4
Requisiti di sicurezza 5
Modularità, flessibilità e standardizzazione 6
Gestione utenze 6
Protezione dati personali 7
Conformità 8
Auditing 8
Portabilità dei dati 9
Accesso del personale addetto 10
Riservatezza 10
Disponibilità del sistema gestionale informatico e SLA 11
Servizi professionali 11
Integrazione con altri sistemi informatici 11
Sistema di gestione dell'autenticazione regionale (SIALI) 12
Servizi professionali di installazione, configurazione, collaudo e messa in produzione del sistema gestionale informatico 14
Servizi professionali di addestramento e formazione del personale 14
Servizio di assistenza e di manutenzione 14
Livelli di servizio (SLA) della assistenza e manutenzione 15
Dimostrazione del sistema gestionale informatico 16
Demo del software 16
Disponibilità accesso web per la valutazione del software 16
Penali 16

L'Aggiudicatario dovrà mettere a disposizione delle Aziende Sanitarie un software gestionale web based per la gestione dell'intero processo di erogazione del servizio di fornitura e distribuzione/consegna degli ausili per incontinenza al domicilio e presso le Case di Riposo (LOTTO 1).

Specifiche non funzionali

Caratteristiche del sistema gestionale informatico

L'Aggiudicatario dovrà garantire l'erogazione delle funzioni del sistema gestionale informatico basato sul modello *cloud computing* in modalità SaaS (*Software as a Service*) a suo carico, conformemente a quanto previsto dalle circolari AgID (Agenzia per l'Italia Digitale) n.2 e n.3 del 09 aprile 2018 per la gestione dell'infrastruttura tecnologica in termini di sicurezza, performance e scalabilità, interoperabilità e portabilità, conformità legislativa, con particolare riferimento alla sicurezza nel trattamento dei dati personali. Pertanto, in adempimento a quanto disposto dall'AgID il sistema informatico utilizzato dovrà essere qualificato e pubblicato nel Cloud Marketplace per la PA di AgID.

La soluzione sarà unica per tutte le Aziende Sanitarie, secondo l'architettura *multi tenant*, garantendo la rigorosa separazione dei dati tra le Aziende Sanitarie.

Se previsto, eventuali accessi di utenti non aziendali, dovranno essere gestiti esclusivamente mediante il sistema pubblico di identità digitale SPID.

Contesto normativo

- Reg. UE n.679/2016 "Nuovo Regolamento Europeo sulla Protezione dei Dati Personali" (GDPR);
- D. Lgs 10 agosto 2018, n. 101 Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);
- D.Lgs 7 marzo 2005, n. 82 e s.m.i (art. 50): "Codice dell'Amministrazione digitale";
- D.Lgs 30 dicembre 2010, n. 235: "Modifiche ed integrazioni al decreto legislativo 7 marzo 2005, n. 82, recante Codice dell'amministrazione digitale, a norma dell'articolo 33 della legge 18 giugno 2009, n. 69";
- Circolare 18 aprile 2017, n. 2/2017 "Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)";
- "Linee guida per lo sviluppo del software sicuro" rilasciate dall'Agenzia per l'Italia Digitale;
- "Linee guida sull'accessibilità degli strumenti informatici" rilasciate dall'Agenzia per l'Italia Digitale;
- Circolari n.2 e n.3 del 09 aprile 2018 dell'Agenzia per l'Italia Digitale;

Requisiti generali

Il sistema gestionale informatico dovrà rispondere ai requisiti obbligatori esplicitati nei prossimi paragrafi. Inoltre dovrà garantire:

- Lingua: utente in lingua italiana; è comunque richiesta la corretta visualizzazione anche dei caratteri diacritici e di altri non appartenenti all'alfabeto latino.

- Privacy e sicurezza: rispetto della normativa vigente in materia di privacy e sicurezza informatica dei dati. La soluzione proposta deve garantire un'adeguata protezione di tutte le informazioni contenute e di tutte le transazioni dati gestite in accordo alla normativa vigente.

e la:

- gestione documentale con la capacità di eseguire l'upload di documenti, anche firmati digitalmente;
- storicizzazione dei dati;
- gestione dei log e la tracciatura delle operazioni nell'iter dei processi. I log devono poter essere storicizzati e archiviati in maniera sicura e inalterabile;
- l'accesso e visibilità dei dati storicizzati a tutte le tipologie di operatori abilitati;
- la manutenibilità;
- la scalabilità.

Le funzioni del sistema gestionale informatico dovranno essere fruibili esclusivamente attraverso un browser web e la soluzione dovrà essere di tipo cross browser, senza alcun ricorso a plugin/estensioni**.**

Data center e connettività

La soluzione dovrà essere erogata da *data center* collegati a una rete di interconnessione a banda larga verso la rete internet senza "single point of failure" ed in grado di garantire connettività a banda piena in Italia ed in particolare verso il datacenter di Insiel SpA, utilizzato dalle Aziende Sanitarie per l'accesso ad Internet e attraverso il quale verranno esposti i servizi per le integrazioni con i sistemi del Servizio Sanitario Regionale.

Per "adeguata" si intende una connettività dimensionata sulla base del bacino di utenza atteso e a garanzia di un tempo di risposta mediamente non superiore, per i processi interattivi ai 10 (dieci) secondi nel 95% dei casi elevato a 15 (quindici) secondi per i processi non interattivi.

Accessibilità ed usabilità

Il sistema gestionale informatico deve possedere caratteristiche d'uso di semplicità, intuitività e omogeneità (essere "user- friendly") anche tramite l'utilizzo di tooltip, icone, messaggi informativi e di avviso.

In merito all'aspetto di usabilità della soluzione, questa dovrà si riportano i criteri segnalati nelle Linee guida di design per i servizi digitali della PA del 23 aprile 2018:

- Percezione: le informazioni e i comandi necessari per l'esecuzione delle attività devono essere sempre disponibili e percettibili.
- Comprensibilità: le informazioni e i comandi necessari per l'esecuzione delle attività devono essere facili da capire e da usare.
- Operabilità: le informazioni e i comandi devono consentire una scelta immediata delle azioni necessarie al raggiungimento dell'obiettivo.
- Coerenza: i simboli, i messaggi e le azioni devono avere lo stesso significato in tutto il sito.
- Tutela della salute: la Piattaforma deve possedere caratteristiche idonee a salvaguardare il benessere psicofisico dell'utente.
- Sicurezza: la Piattaforma deve possedere caratteristiche idonee a fornire transazioni e dati affidabili, gestiti con adeguati livelli di sicurezza.

- Trasparenza: la Piattaforma deve comunicare all'utente lo stato, gli effetti delle azioni compiute e le informazioni necessarie per la corretta valutazione delle modifiche effettuate sul sito stesso.
- Facilità di apprendimento: l'applicativo deve possedere caratteristiche di utilizzo di facile e rapido apprendimento.
- Aiuto e documentazione: le funzionalità di aiuto, quali le guide in linea e la documentazione sul funzionamento dell'applicativo devono essere di facile reperimento e collegate alle azioni svolte dall'utente.
- Tolleranza agli errori: la Piattaforma deve essere configurato in modo da prevenire gli errori; ove questi, comunque, si manifestino, occorre segnalarli chiaramente e indicare le azioni necessarie per porvi rimedio.
- Gradevolezza: la Piattaforma deve possedere caratteristiche idonee a favorire e a mantenere l'interesse dell'utente.
- Flessibilità: la Piattaforma deve tener conto delle preferenze individuali e dei contesti.

In merito all'aspetto accessibilità si rimanda alle linee guida AGID sull'accessibilità degli strumenti informatici rilasciate in data 26/11/2019. Inoltre il sistema gestionale informatico dovrà inoltre rispettare le norme di accessibilità così come stabilito dalla Legge 9 gennaio 2004 n. 4 e ss.mm. (c.d. "legge Stanca") e del successivo Decreto del Presidente della Repubblica, 1 marzo 2005, n. 75 "Regolamento di attuazione della legge 9 gennaio 2004, n. 4 per favorire l'accesso dei soggetti disabili agli strumenti informatici".

L'interfaccia utente sarà personalizzata per essere il più possibile user friendly, allo scopo di consentire un'utile ed efficiente gestione dei documenti e dei processi ed una rappresentazione chiara ed esaustiva dei dati. A tal proposito il sistema gestionale informatico dovrà dimostrare un'adeguata progettazione e realizzazione al fine di garantire:

- un'interfaccia grafica intuitiva,
- menù e funzionalità comprensibili,
- icone ben definite, leggibili e ben posizionate nelle varie form/pagine,
- la presenza di tutorial e didascalie vicino alle varie voci del programma.

Requisiti di sicurezza

Il sistema gestionale informatico dovrà essere adeguato al Regolamento Ue 2016/679, noto come GDPR (General Data Protection Regulation), relativo alla protezione delle persone fisiche con riguardo al trattamento e alla libera circolazione dei dati personali.

Inoltre, le misure minime di sicurezza ICT emanate dall'AgID, rappresentano un riferimento pratico utile a valutare e migliorare il livello di sicurezza informatica, al fine di contrastare le minacce informatiche più frequenti. Le misure sono state classificate come "Minime" (ogni PA deve necessariamente essere o rendersi conforme), "Standard" (ogni PA deve considerare come base di riferimento), "Avanzato" (visto come obiettivo di miglioramento).

A titolo puramente esemplificativo e non esaustivo è richiesto che il sistema gestionale informatico garantisca:

- i requisiti di riservatezza, autenticità, integrità, disponibilità e non ripudio. Devono essere disponibili adeguate tecnologie antivirus;
- l'utilizzo di connessioni geografiche esclusivamente sicure, anche in termini di disponibilità e di performance, oltre che di idonei meccanismi d'autenticazione e autorizzazione; l'accesso ai sistemi dovrà essere vincolato da password criptate e non decifrabili nemmeno dagli amministratori di sistema, rispondenti ai requisiti posti dalla normativa vigente;
- l'utilizzo di meccanismi di identificazione degli utenti e autorizzazione all'accesso e tutte le fasi di autenticazione (user login), inclusi i processi di autenticazione forte mediante soluzioni in grado di gestire certificati di autenticazione emessi da Enti certificatori legalmente riconosciuti (smart-card, token, ecc.);
- l'adozione di appositi sistemi di tracciamento e registrazione a livello di sistema (log applicativi) delle attività eseguite da tutti gli utenti del sistema, siano essi interni od esterni, e compresi gli utenti di amministrazione in accordo alla normativa vigente. Questi sistemi dovranno consentire la parametrizzazione della durata di tenuta dei file log generati secondo le indicazioni impartite dalla Stazione Appaltante;
- il trattamento dei dati sensibili in pieno accordo alle normative vigenti in materia.

L'Aggiudicatario dovrà inoltre garantire che la soluzione proposta sia stata progettata e realizzata adottando delle politiche per lo sviluppo sicuro del codice secondo quanto dettato dalle "Linee guida per lo sviluppo del software sicuro" rilasciate da AgiD.

Pertanto la soluzione dovrà essere fornita adottando tutti gli accorgimenti necessari atti ad evitare l'introduzione di vulnerabilità tecniche nel software stesso.

Le Aziende Sanitarie si riservano la possibilità di effettuare delle verifiche sulla sicurezza dei sistemi messi in campo dall'Aggiudicatario.

L'Aggiudicatario è responsabile per danni o violazioni dei dati connessi ad accertate vulnerabilità del software stesso e si impegna a correggere prontamente qualsiasi vulnerabilità software che gli venisse segnalata o di cui venisse a conoscenza considerando tale evento alla pari di un guasto bloccante e pertanto con gli stessi SLA previsti nel presente documento.

Modularità, flessibilità e standardizzazione

Il sistema gestionale informatico dovrà essere strutturato per moduli integrati, affinché tutte le informazioni siano rese automaticamente disponibili tra i diversi moduli oltre che prevedere la massima rispondenza alle diverse esigenze di interoperabilità.

Le varie componenti del sistema dovranno essere modulari e progettate in modo tale da garantire l'implementazione di ulteriori moduli e/o plug-in oltre all'integrazione con altri sistemi. I componenti dovranno essere in grado di adeguarsi ai mutamenti tecnologici ed all'interazione con altri progetti. Deve essere prevista la massima flessibilità della soluzione proposta in termini di scalabilità tecnologica al fine di garantire il pronto e completo supporto sia agli aggiornamenti normativi sia di tipo funzionale e dimensionale richiesti dalle Aziende Sanitarie dovute alle mutate esigenze in termini di numero di utenti e di funzioni applicative.

Gestione utenze

Il sistema gestionale informatico dovrà avere un sistema integrato di gestione di tutte le tipologie di utenze con la possibilità di operare per la creazione, modifica ed eliminazione di utenti. L'accesso

all'applicazione da parte dei vari utenti per le diverse funzionalità disponibili deve essere regolato mediante la creazione di adeguati ruoli e specifici privilegi per ciascun ruolo. Ogni ruolo deve essere configurato con un diverso insieme di diritti che determinano il particolare accesso alle informazioni e attività del sistema.

Per quanto riguarda le sole utenze riferite agli operatori delle Aziende Sanitarie, il sistema gestionale informatico dovrà integrarsi con il sistema regionale SIALI per l'autenticazione e l'autorizzazione centralizzata delle applicazioni in Sanità.

La gestione del ciclo di vita delle credenziali applicative per le utenze non riferite agli operatori delle Aziende Sanitarie sarà a carico dell'Aggiudicatario. Le utenze applicative sono nominali e le credenziali sono erogate dall'Aggiudicatario secondo un percorso definito e sicuro che tenga separate username e password, in modo che sia possibile:

- definire la complessità della password secondo le migliori pratiche (lunghezza, maiuscole/minuscole e caratteri speciali);
- la gestione di più profili utente con privilegi di autorizzazione diversi; sulla base delle credenziali fornite dall'utente, si devono individuare i diritti e le autorizzazioni che l'utente possiede e permetterne l'accesso alle risorse limitatamente a tali autorizzazioni, in modo che l'utente abbia accesso alle sole risorse relative all'attività che deve svolgere, secondo il concetto di minimizzazione;
- la funzionalità di "richiesta creazione o cambio della password al primo accesso";
- il blocco dell'utenza dopo un numero definito (fisso o variabile) di tentativi falliti di accesso;
- registrare gli accessi degli utenti in un archivio (log) non cancellabile con il reset;
- gestire i log di sistema (accessi, allarmi, ecc.).

Per quanto concerne gli "*account amministrativi*" (ovvero ogni account a cui è associato un ruolo Amministratore o che è dotato di privilegi amministrativi o che consenta di svolgere funzioni di amministratore su qualunque macchina, sistema o applicativo fornito), questi sono gestiti a cura e responsabilità della Ditta Fornitrice, seguendo le norme e le migliori pratiche in materia.

Protezione dati personali

Il sistema gestionale informatico dovrà gestire dati dei cittadini del Friuli Venezia Giulia. I Titolari dei dati sono pertanto le singole Aziende Sanitarie. Ciascuna Azienda Sanitaria, in qualità di "Titolare del trattamento dei dati personali", nominerà l'Aggiudicatario "Responsabile del trattamento" ai sensi del Regolamento UE 2016/679, specificando analiticamente per iscritto i compiti dello stesso e vigilando periodicamente sulla puntuale osservanza delle istruzioni impartite e sul generale rispetto della normativa italiana ed europea in materia di protezione dei dati personali.

Risultano inclusi nella titolarità delle singole Azienda sanitarie i dati presenti nel sistema gestionale informatico nonché le ulteriori informazioni relative ai servizi gestiti. L'Aggiudicatario è autorizzato alla loro gestione esclusivamente per le necessità ed i fini previsti dal presente appalto, e nel rispetto della normativa vigente.

I dati devono essere trattati nel territorio dell'Unione Europea ed essere archiviati esclusivamente in tale Area Geografica, senza possibilità di loro trasferimento in territorio extra Unione Europea.

Il sistema gestionale informatico dovrà prevedere, in ottemperanza di disposizioni e/o provvedimenti normativi, meccanismi di autenticazione, autorizzazione e profilatura per l'accesso alle funzionalità previste, ai dati e ai file trattati.

Dovrà essere assicurata la gestione di dati personali, per i quali dovrà essere garantita una soluzione che comporti il pieno rispetto della normativa generale e della ulteriore normativa di settore applicabile.

Poiché i dati da gestire rivestono carattere di estrema importanza per quanto concerne gli aspetti legati alla privacy viene pertanto richiesto di assicurare, per ogni singolo elemento richiesto e per il servizio nel suo insieme, l'utilizzo di processi, strumentazioni e personale tali da garantire la sicurezza e la protezione dei dati nel rispetto della vigente normativa e di rispondere ai requisiti di seguito dettagliati.

Conformità

L'Aggiudicatario dovrà garantire che il trattamento dei dati gestiti per conto del Titolare, sarà effettuato in piena conformità a quanto previsto dal GDPR.

In relazione alle disposizioni di cui al Regolamento UE 2016/679 l'Aggiudicatario, previa effettuazione dell'analisi dei rischi (e tenendo conto, in particolare, dei rischi che derivano dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, ai dati personali trasmessi, conservati o comunque trattati), dovrà individuare ed adottare misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, tenendo conto, fra l'altro, della tipologia di trattamento, delle finalità perseguite, del contesto e delle specifiche circostanze in cui avviene il trattamento, nonché della tecnologia applicabile e dei costi di attuazione. Tali misure comprendono:

- la pseudonimizzazione e la cifratura dei dati personali laddove è opportuno;
- la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico.

Auditing

L'Aggiudicatario ammette la possibilità da parte delle Aziende Sanitarie di effettuare delle verifiche circa il rispetto delle politiche di sicurezza delle informazioni codificate. In particolare, l'Aggiudicatario, ammette la possibilità da parte delle Aziende Sanitarie di effettuare attività di monitoraggio e riesame dei servizi forniti.

L'Aggiudicatario si impegna altresì a:

- attenersi, per quanto sia rilevante in relazione alle attività definite nel presente contratto, al rispetto di tutte le previsioni, almeno di livello Standard, previste dalla Circolare dell'Agenzia per l'Italia Digitale 18 aprile 2017, n. 2/2017 Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante: «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)»;

- condurre periodicamente test per garantire la conformità alle indicazioni ricevute, inclusi gli obblighi di riservatezza, non divulgazione, sicurezza e di porre i risultati alla consultazione di ciascuna Azienda Sanitaria, su richiesta;
- informare prontamente il Titolare di ogni questione rilevante ai fini di legge, in particolar modo, a titolo esemplificativo e non esaustivo, nei casi in cui abbia notizia, in qualsiasi modo, che risulti violata la normativa in materia di protezione dei dati personali, ovvero che il trattamento presenti rischi specifici per i diritti, le libertà fondamentali e/o la dignità dell'interessato, nonché qualora, a suo parere, un'istruzione violi la normativa, nazionale o comunitaria, relativa alla protezione dei dati;
- collaborare, se richiesto dal Titolare, con altri soggetti, al fine di armonizzare e coordinare l'intero processo di trattamento di dati e informazioni, in relazione alle attività di cui al presente contratto;
- mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al contratto e consentire alle Aziende Sanitarie l'esercizio del potere di controllo e ispezione, prestando ogni necessaria collaborazione alle attività di audit effettuate dalle Aziende Sanitarie stesse o da un altro soggetto da questi incaricato o autorizzato, con lo scopo di controllare l'adempimento degli obblighi e delle istruzioni di cui al presente contratto. Resta inteso che qualsiasi verifica condotta ai sensi del presente comma dovrà essere eseguita in maniera tale da non interferire con il normale corso delle attività dell'Aggiudicatario e fornendo a quest'ultimo un ragionevole preavviso;
- una procedura adeguata (messa a disposizione del Titolare su richiesta) per provare, verificare e valutare regolarmente l'efficacia delle misure adottate al fine di garantire la sicurezza del trattamento.

Portabilità dei dati

In previsione della cessazione del rapporto contrattuale, l'Aggiudicatario dovrà fornire il supporto necessario per agevolare la migrazione dei dati verso altro operatore:

- produrre e fornire tutti gli elementi necessari alle Aziende Sanitarie e/o al nuovo operatore al fine di una corretta migrazione dei servizi verso una nuova infrastruttura;
- fornire la piena e corretta collaborazione con le Aziende Sanitarie e il nuovo eventuale operatore, operando nel rispetto dei rapporti tra le parti e delle indicazioni impartite dalle Aziende Sanitarie;
- mettere a disposizione la documentazione, diagrammi e tutti gli elementi utili a descrivere la soluzione ed i dati presenti, rendendoli disponibili, in lingua italiana, nei formati aperti richiesti dalle Aziende Sanitarie;
- garantire la totale continuità del servizio fino alla messa in produzione della nuova piattaforma del nuovo operatore individuato, secondo le tempistiche che verranno concordate tra le parti;
- garantire la conservazione e l'accesso ai dati per tutta la durata delle operazioni di migrazione e
- messa in produzione della piattaforma sulla nuova infrastruttura.

Le attività di migrazione e consegna dei dati e chiusura del servizio saranno documentate attraverso verbali sottoscritti tra le parti.

Una volta consegnati i dati da migrare, il fornitore provvede alla disattivazione del servizio e, terminato il periodo di salvaguardia di 120 giorni solari, all'eliminazione definitiva dei dati dai sistemi e dai supporti di backup e disaster recovery.

In ogni momento le Aziende Sanitarie potranno comunque richiedere all'Aggiudicatario, con un preavviso di almeno tre giorni, di effettuare lo scarico non oneroso di tutti i dati del sistema sul supporto rimovibile e in un formato aperto e adeguatamente documentato.

Accesso del personale addetto

L'Aggiudicatario dovrà garantire la tracciatura (in ossequio al provvedimento del Garante Privacy del 27 novembre 2008 recante "Misure e accorgimenti, prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" e successive modifiche), anche completa, di tutti gli accessi, tentativi di accesso e delle attività svolte sui sistemi nell'ambito del presente contratto da parte dei soggetti abilitati ad operare in qualità di Amministratori di Sistema. Tale tracciatura potrà comprendere anche gli accessi falliti o altre casistiche di errore, anche se non espressamente previste.

L'Aggiudicatario si impegna a fornire ai Titolari le evidenze dell'accesso degli Amministratori di Sistema, a semplice richiesta e coerentemente con i requisiti di *retention* definiti dal provvedimento sopra citato.

Riservatezza

L'Aggiudicatario tutelerà la piena riservatezza delle informazioni acquisite nell'esecuzione del presente contratto, rispettando le seguenti clausole di riservatezza (NDA - *Non Disclosure Agreement*) ed in particolare si obbliga a:

- considerare e trattare in maniera strettamente riservata tutte le informazioni, dati o documenti ricevuti o resi accessibili dai Titolari e ad attuare tutte le cautele e le misure di sicurezza necessarie e opportune, secondo i migliori standard professionali, al fine di mantenere riservate tali informazioni e prevenire accessi non autorizzati, la sottrazione e la manipolazione delle stesse;
- non divulgare e/o comunque a non rendere note a Terzi le informazioni, intendendosi per "Terzi" tutti i soggetti diversi dagli amministratori, dipendenti, intermediari o consulenti ("Persone Collegate") delle Aziende Sanitarie, a cui l'Aggiudicatario potrà comunicare le informazioni nella misura in cui ciò sia necessario al fine di consentirgli di svolgere le attività affidategli.

In ogni caso, i documenti e i dati trattati dall'Aggiudicatario non potranno essere neanche parzialmente duplicati, riprodotti, esportati, comunicati a terzi, né diffusi o trasferiti al di fuori dell'Unione Europea e sempre e comunque dovranno essere trattati nell'esatta osservanza degli obblighi contrattuali e delle finalità ricomprese nelle obbligazioni assunte dall'Aggiudicatario con il presente contratto.

L'Aggiudicatario si impegna, altresì, a redigere (e a comunicare) una lista delle persone autorizzate a trattare i dati dei Titolari e adottare procedure documentate e verificabili per prevenire l'accesso a tali dati da parte di persone non autorizzate.

Qualora la diffusione presso terzi di materiale, dati, documenti o di informazioni sia stato causato da atti o fatti direttamente imputabili all'Aggiudicatario e/o ai loro dipendenti, quest'ultimo sarà tenuto a risarcire ai Titolari interessati gli eventuali danni connessi alla violazione dell'obbligo di riservatezza.

L'Aggiudicatario si impegna ad erogare i servizi di gestione oggetto della presente fornitura limitando il più possibile l'accesso ai dati personali contenuti nei sistemi oggetto della presente fornitura.

Disponibilità del sistema gestionale informatico e SLA

L'Aggiudicatario dovrà garantire il funzionamento del sistema gestionale informatico 24 ore al giorno, 7 giorni alla settimana, 365 giorni all'anno, salvo i periodi di interruzione del servizio per attività di manutenzione. Inoltre dovrà fornire garanzia di *business continuity* con la definizione di opportuni livelli di servizio per un *uptime* di almeno il 99% per l'ambiente di produzione.
Si precisa che nel calcolo della disponibilità del servizio non saranno considerate interruzioni dovute ad eventi di forza maggiore, intesi come eventi imprevisti ed imprevedibili, al di fuori del controllo dell'Aggiudicatario, o interruzioni concordate con le Aziende Sanitarie dovute ad interventi manutentivi programmati.

Servizi professionali

L'Aggiudicatario dovrà erogare i servizi professionali per:

- installazione, configurazione, collaudo e messa in produzione del sistema gestionale informatico;
- addestramento e formazione del personale;
- assistenza e manutenzione;
- progettazione, sviluppo e realizzazione delle integrazioni del software con i sistemi informatici del Sistema Sanitario Regionale che dovessero essere integrati, oltre alle riconfigurazioni e migrazioni dati nel caso di eventuali riorganizzazioni dell'assetto delle Aziende Sanitarie nel caso di riforme del Sistema Sanitario Regionale medesimo;

Integrazione con altri sistemi informatici

Il Sistema Informativo Aziendale (SIA) delle Aziende Sanitarie del Friuli Venezia Giulia è prevalentemente costituito, allo stato dell'arte, da applicazioni/soluzioni fornite da Insiel SpA nell'ambito del SISSR (*Sistema Informativo Socio Sanitario Regionale* della Regione Friuli Venezia Giulia) o acquisiti su mandato della Direzione Centrale Salute, Politiche Sociali e Disabilità della regione Friuli Venezia Giulia, integrati al SIA, forniti e gestiti, in tutto o in parte, da terze parti.

Durante l'esecuzione del contratto, le Aziende Sanitarie, per il tramite di ARCS, potranno decidere di integrare il sistema gestionale informatico con altri sistemi informatici del SISSR, al fine di riutilizzare in maniera bidirezionale i dati con il sistema gestionale informatico.

Possibili scenari di integrazione sono individuabili al momento con i seguenti sistemi informatici:

1. gestione dell'autenticazione regionale (SIALI);
2. gestione distretti sanitari;
3. gestione economato-magazzino-contabilità aziendale;

Si tratta di un elenco non esaustivo.

Sulla base della richiesta delle Aziende Sanitarie, per il tramite di ARCS, l'Aggiudicatario dovrà formulare un progetto per la realizzazione dell'integrazione del sistema gestionale informatico con i sistemi regionali attraverso opportune Application Programming Interface (API) di tipo SOAP e/o REST che verranno messe a disposizione e documentate da parte di Insiel SpA, e saranno fruibili attraverso il *datacenter* della medesima. Le integrazioni dovranno essere sviluppate e rese operative dall'Aggiudicatario quanto prima, entro 3 mesi dalla richiesta del progetto.

Qualora dovesse verificarsi la necessità di riorganizzare le Aziende Sanitarie a seguito di un provvedimento normativo di riforma sanitaria, l'Aggiudicatario dovrà predisporre un piano di migrazione per riconfigurare il sistema gestionale informatico in modo da attuare quanto previsto dalla riforma, entro 3 mesi dalla richiesta di riorganizzazione.

Sistema di gestione dell'autenticazione regionale (SIALI)

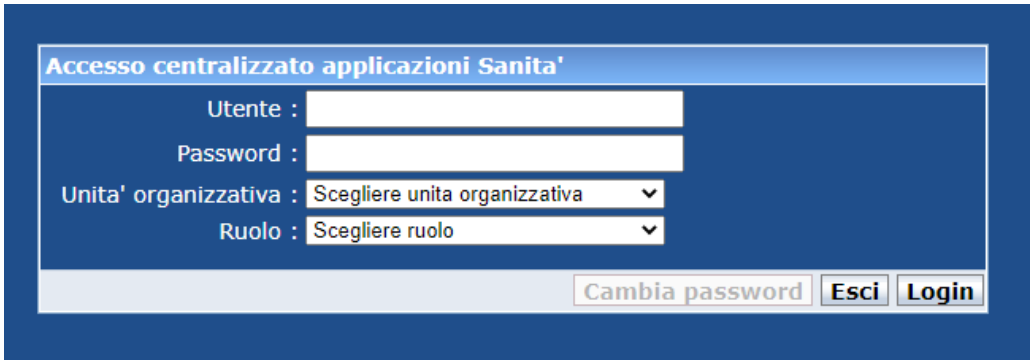
Per le sole utenze riferite alle attività svolte dalle Aziende Sanitarie, il sistema gestionale informatico dovrà garantire l'integrazione con il sistema regionale SIALI per l'autenticazione e l'autorizzazione centralizzata delle applicazioni in Sanità.

Siali è una componente software per la gestione del SSON, che a fronte della corretta autenticazione dell'utente rilascia un ticket per l'interazione con gli altri componenti applicativi del sistema FVG (Anagrafe, ADT, Gestore Richieste,...), e per l'accesso ai dati nel contesto clinico ospedaliero.

La componente è integrabile per mezzo di servizi SOAP, per la generazione/gestione del ticket.

Per la fase di autenticazione dispone di due modalità possibili:

1) Chiamata in contesto: Disegnata per l'utilizzo da sistemi terzi realizzati in modalità web. Fornisce una pagina web di login (con gestione di modifica/cambio password) con la quale eseguire direttamente l'accesso. Si riporta a titolo di esempio l'immagine della pagina web di login.



Al termine della fase di login viene passato il ticket al sistema chiamante di terze parti, utilizzando la redirect uri indicata nei parametri di invocazione della pagina di login.

2) Utilizzo di WebService SOAP, più indicata per i sistemi terzi che non utilizzano modalità web. La fase di autenticazione richiede i seguenti step:
   1) Richiesta del ticket: restituisce un ticket propedeutico alla fase di autenticazione.
   2) Autenticazione:

a. la fase di autenticazione viene effettuata invocando un web service al quale vengono passate le credenziali di accesso definite a livello di sistema centrale (utente, password, applicazione, …) e il certificato SIALI richiesto in precedenza,
b. se l'operazione va a buon fine viene ritornato un elenco di informazioni a cui l'utente è abilitato in funzione del login effettuato (lista dei ruoli, lista strutture, lista applicazioni, lista funzioni abilitate). In caso negativo, viene ritornato un messaggio contenente il motivo dell'esito negativo,
c. una volta effettuata l'autenticazione è possibile procedere all'invocazione dell'applicativo desiderato (anche chiamate ad ulteriori applicativi sanità), secondo le specifiche dell'applicativo stesso, includendo il riferimento al certificato SIALI richiesto in precedenza.

Fornisce inoltre i seguenti servizi SOAP di supporto:

1. Cambio password utente,
2. Logout: al termine dell'utilizzo dell'applicazione chiamante (ad es. alla chiusura dell'applicativo) va effettuato il logout da SIALI relativamente al certificato che si sta usando,
3. Servizi di verifica validità del ticket e abilitazioni associate.

Tutti i servizi e le chiamate in contesto prevedono l'utilizzo di protocollo https.

Le specifiche tecniche di dettaglio relativamente ai servizi elencati, e le relative modalità di chiamata verranno fornite a valle della aggiudicazione, cosi come verrà analizzato lo scenario di utilizzo più opportuno per la fase di autenticazione e le relative configurazioni necessarie nel sistema configuratore SISR.

L'integrazione descritta rappresenta l'attuale implementazione del sistema SSON, e può essere soggetta a revisione ed evoluzione in futuro: dovrà comunque essere garantita l'integrazione con le eventuali revisioni.

Il sistema gestionale informatico dovrà gestire l'accesso alle diverse funzionalità da parte degli operatori delle Aziende Sanitarie sulla base dei profili di accesso di seguito indicati e i livelli di accesso a seconda dei gruppi di appartenenza indicati nel seguente elenco esemplificativo e non esaustivo:

- PRE: medico prescrittore
- RIA: riabilitatore
- INF: infermiere
- UAP: Ufficio Assistenza Protesica
- AFIR UFFICIO ASSISTENZA FARMACEUTICA INTEGRATIVA REGIONALE (che autorizza i presidi di incontinenza)
- BEN: Beni e Servizi
- DIR: Direzione Sanitaria
- MGD: Magazzino Distretto

Ciascuna Azienda Sanitaria dovrà essere in grado di gestire le utenze riferite ai profili di accesso di pertinenza.

Servizi professionali di installazione, configurazione, collaudo e messa in produzione del sistema gestionale informatico

L'Aggiudicatario dovrà prevedere un piano di avviamento dettagliato e completo, definito per ciascuna azienda sanitaria, che consenta di arrivare alla messa in produzione del sistema nel pieno rispetto dei requisiti descritti nel presente capitolato. In fase di offerta tecnica il Concorrente dovrà descrivere il percorso più opportuno illustrandone modalità, contenuti, persone dedicate e durata.

L'Aggiudicatario dovrà garantire lo svolgimento, senza oneri aggiuntivi per le Aziende Sanitarie, di tutte le attività di configurazione e personalizzazione del sistema per una corretta aderenza delle funzionalità, di cui al presente documento, alle realtà specifiche di ciascuna delle Aziende Sanitarie.

Sarà inoltre onere dell'Aggiudicatario garantire, per l'intera durata delle fasi di installazione e configurazioni varie di avviamento presso le Aziende Sanitarie, la presenza del proprio Referente o del proprio team di lavoro agli incontri che si renderanno necessari.

Dovrà essere previsto un ambiente di test, separato dall'ambiente di produzione (in modo da non alterarne le performance), con accessibilità garantita a tutti i livelli di utenza previsti. L'Aggiudicatario si impegna, con oneri a proprio carico e per l'intera durata del contratto, a garantire l'allineamento dei due ambienti per i test ed il rilascio di eventuali aggiornamenti applicativi.

Servizi professionali di addestramento e formazione del personale

Le attività di addestramento e formazione dovranno essere svolte dall'Aggiudicatario contestualmente all'avviamento del sistema gestionale informatico, presso le sedi delle Aziende Sanitarie, secondo date e orari che verranno concordate in fase di avviamento, con l'obiettivo di raggiungere la completa padronanza del sistema gestionale informatico ai fini dell'erogazione ottimale del servizio.

La formazione dovrà essere erogata da personale che abbia un'ottima conoscenza del sistema e sia dotato di capacità ed attitudine a gestire i rapporti interpersonali.

Sarà onere dell'Aggiudicatario fornire prima dell'avvio delle sessioni formative, secondo modalità e contenuti concordati tra le parti, tutto il materiale (es. manuali d'uso, programma del corso, tutorial video, ecc..) richiesto sia in formato cartaceo ed elettronico.

Servizio di assistenza e di manutenzione

Il servizio potrà essere richiesto tramite apposito sistema di ticketing accessibile via web in grado di gestire, documentare e monitorare gli interventi di assistenza richiesti (tempi di chiusura, segnalazioni, azioni intraprese, risoluzione e evasione, ecc.). In alternativa all'accesso diretto via web, l'apertura dei ticket potrà essere effettuata anche attraverso un numero di telefono messo a disposizione dell'Aggiudicatario, attivo durante le ore di ufficio.
I dati del sistema di ticketing verranno utilizzati per la produzione di report a fini documentativi e di verifica di conformità nell'erogazione del servizio richiesto rispetto agli SLA stabiliti. L'Aggiudicatario dovrà fornire alle Aziende Sanitarie l'accesso in consultazione al sistema di ticketing ad utenti indicati da ciascuna Azienda Sanitaria.

L'attività di manutenzione dovrà garantire, oltre al normale e regolare funzionamento delle procedure, anche la diagnosi e la rimozione delle cause e degli effetti dei malfunzionamenti e/o del degrado delle prestazioni del sistema nel suo complesso, le attività di back up, il ripristino di dati e le configurazioni; dovrà essere inoltre inclusa la manutenzione normativa, necessaria per apportare

modifiche e/o aggiornamenti che si rendessero necessari a seguito di variazioni legislative e/o normative a livello regionale, nazionale e/o internazionale, nonché tutte le attività e gli interventi necessari a garantire la costante aderenza della soluzione all'evoluzione dell'ambiente tecnologico del sistema informativo e al cambiamento dei requisiti organizzativi.

L'Aggiudicatario dovrà garantire per tutta la durata del contratto d'appalto:

- la rimozione di errori bloccanti e la risoluzione di eventuali malfunzionamenti;
- la risoluzione di eventuali malfunzionamenti, con tempi di risoluzione diversificati in funzione del livello di gravità e nel pieno rispetto degli SLA;
- la risposta alle richieste di supporto operativo utilizzo delle funzionalità applicative.

Qualunque rilascio o aggiornamento del sistema dovrà avvenire con modalità e orari tali da ridurre al minimo il disservizio e dovrà essere sempre e comunque concordato con le Aziende Sanitarie.

Il servizio di assistenza deve esser erogato tutti i giorni lavorativi

- dal lunedì al venerdì dalle ore 08.00 alle ore 18.00
- il sabato dalle ore 08.00 alle ore 12.00

da personale dell'Aggiudicatario con competenze idonee alla risoluzione di eventuali malfunzionamenti e nel rispetto degli SLA.

Livelli di servizio (SLA) della assistenza e manutenzione

Il servizio di assistenza e manutenzione in garanzia deve essere erogato nel pieno rispetto dei livelli di servizio di seguito descritti. Si identificano 4 tipologie di eventi:

- guasto bloccante: qualunque tipo di guasto che preclude del tutto o in parte l'operatività del sistema gestionale informatico;
- guasto limitante: qualunque tipo di guasto che preclude alcune funzionalità del sistema gestionale informatico anche se non impatta l'operatività;
- guasto non limitante: qualunque tipo di guasto che non preclude nessuna funzionalità del sistema gestionale informatico né impatta l'operatività;
- richiesta di supporto operativo utilizzo delle funzionalità applicative.

La verifica degli SLA verrà applicata su base semestrale e prenderà in considerazione tutti gli interventi di manutenzione tecnica chiusi nel periodo esaminato anche se aperti in periodi di osservazione precedenti. Verrà calcolato il Tempo di Risoluzione che dovrà risultare, per almeno il 90% dei casi esaminati, inferiore al Tempo di Risoluzione Massimo (TRisMax) espresso nella tabella seguente per singola tipologia di evento.

Tipo di evento	**TRisMax** **Tempo di Risoluzione**
Bloccante	4 h solari
Limitante o richiesta di supporto operativo	8 h lavorative
Non limitante	40 h lavorative

Il Tempo di Risoluzione (TRis) sarà calcolato come segue:

$$TRis = Tc - Ti$$

dove:

- Ti: è il tempo di inizio dell'intervento, che coincide con l'istante in cui verrà fatta comunicazione all'Aggiudicatario del malfunzionamento da parte delle Aziende Sanitarie;
- Tc: è il tempo di chiusura dell'intervento, che coincide con l'istante in cui verrà effettivamente risolto il guasto.

Un guasto si considera aperto fino alla completa risoluzione e ripristino della funzionalità. Un guasto Bloccante risolto tramite workaround può essere riclassificato come Limitante o Non limitante, o in alternativa può essere aperto un nuovo ticket, e concorre comunque all'analisi degli SLA relativi.

Il mancato rispetto dei livelli di servizio sopra riportati sarà oggetto di penali.

Dimostrazione del sistema gestionale informatico

Demo del software

Il concorrente dovrà organizzare presso la sede della stazione appaltante una sessione dimostrativa del software proposto. La dimostrazione dovrà rispettare un tempo massimo di ~~tre~~ ore per concorrente e potrà essere interrotta da richieste di chiarimenti verbali da parte della commissione.

La stazione appaltante metterà a disposizione dei concorrenti un locale attrezzato con postazione di lavoro, dotata di browser e abilitata al collegamento a internet. Eventuali altre apparecchiature ed il software necessari alla dimostrazione saranno a carico del concorrente.

L'indicazione della sede, la data e l'ora della dimostrazione saranno comunicati ad ogni concorrente via PEC o al numero di fax indicato nella domanda di partecipazione almeno 72 ore prima dello svolgimento della dimostrazione stessa.

Disponibilità accesso web per la valutazione del software

L'impresa durante la fase di valutazione delle offerte tecniche dovrà rendere disponibile alla commissione l'accesso ad un sistema già configurato al solo scopo di agevolare la valutazione funzionale del prodotto, con funzionalità complete e abilitate all'uso. Nel caso di necessità, la Commissione potrà chiedere chiarimenti entro un termine congruo fissato dalla Commissione stessa.

Penali

L'Azienda Sanitaria in caso di inadempimenti dell'Aggiudicatario applicherà le seguenti penali:

Relativamente all'esecuzione dei servizi di assistenza di II livello e manutenzione in garanzia di cui

al paragrafo "Livelli di servizio (SLA) della assistenza e manutenzione", il mancato rispetto dei termini comporterà l'applicazione di una penale pari ad Euro 500,00 (cinquecento/00) per ogni punto percentuale in difetto del valore TRis, calcolato nel periodo di osservazione come meglio indicato nel succitato paragrafo, fatto salvo il maggior danno.

Per tutto quanto non previsto nel presente documento si fa espresso riferimento alle specifiche IT di ogni singola Azienda Sanitaria aderente al servizio.