ALLEGATO TECNICO

Telemonitoraggio pazienti COVID-19

Sommario

1. OGGETTO DELLA FORNITURA

Oggetto della presente Fornitura consiste nell'erogazione di un servizio di Telemonitoraggio per i pazienti COVID-19 in isolamento domiciliare. Il servizio ha l'obiettivo di consentire ai Medici di Medicina Generale (MMG) ed ai medici delle strutture sanitarie di ridurre il numero di contatti con i pazienti ad alto rischio, riducendo allo stesso tempo la possibilità da parte dei pazienti di entrare in contatto, proprio presso le strutture di assistenza, con il virus e quindi con forme di contagio.

Il servizio risponde, inoltre, non solo ai pazienti COVID-19 positivi, ma anche a quelli non ancora testati che hanno sintomatologia influenzale riconducibile a COVID-19. Il sistema, inoltre, potrebbe essere esteso anche a pazienti cronici e fragili che potrebbero, in caso di contagio, vedere aggravarsi la propria condizione di salute fino a renderla a "rischio vita". Proprio per questi ultimi pazienti vi è la necessità di maggior accesso al servizio sanitario, ma senza doverli esporre al contatto fisico in un luogo che è da considerarsi in questo momento ad alto rischio.

La soluzione proposta consentirà di effettuare la sorveglianza clinica delle condizioni del paziente, in raccordo con i MMG e i medici delle strutture sanitarie e, in alcuni casi, di monitorare anche l'andamento di alcuni parametri clinici misurati con dispositivi messi nell'ambito della fornitura a disposizione del paziente.

Infine, il servizio risponde alla necessità di tutelare la sicurezza e la salute del personale medico ed infermieristico, consentendo di affiancare all'attuale protezione fisica tramite presidi, che pure scarseggiano, una protezione attiva che riduca drasticamente le occasioni di contatto.

Quanto sopra premesso, il servizio oggetto della fornitura, dettagliato nel Capitolo 4, si articola in:

- un insieme di componenti tecnologiche costituito da una Piattaforma Applicativa, Kit di Telemonitoraggio ed eventuale strumentazione messa a disposizione degli MMG per la raccolta, l'elaborazione e gestione dei dati;
- un Centro di Supporto Tecnologico per la gestione delle componenti tecnologiche e relativo supporto agli utilizzatori;
- una Centrale Medica per il supporto agli MMG e Medici Ospedalieri nella gestione della sorveglianza attiva dei pazienti ove non già svolta da cooperative o strutture territoriali presenti.

2. STRATEGIA DI SOURCING

La **strategia di realizzazione** prevede la selezione di più **Fornitori** ognuno operante su una area territoriale predefinita a cui affidare l'erogazione del servizio nel suo complesso che possano dimostrare di possedere i requisiti tecnici e di esperienza specifica maturata e di essere in grado di attivare immediatamente il servizio.

È importante specificare, che i pazienti serviti da un Fornitore potranno essere affidati a giudizio della Stazione Appaltante agli altri Fornitori aggiudicatari, in caso di:

- fault tecnologico del Fornitore, interscambiabilità e continuità del servizio;
- incapacità del Fornitore a garantire i Livelli di Servizio richiesti.

Ogni Fornitore aggiudicatario dovrà quindi garantire la capacità di scalare l'erogazione dei propri servizi.

3. PROCESSO DI RIFERIMENTO

Gli **attori coinvolti** nel servizio sono:

- i Medici di Medicina Generale (di seguito MMG);
- i Medici delle strutture sanitarie dimettenti (di seguito Medico Ospedaliero);
- gli operatori degli erogatori ADI;
- gli operatori della unità speciale di Continuità Assistenziale appositamente costituita (di seguito Operatore CA);
- la Centrale Medica;
- il Centro Supporto Tecnologico del Fornitore;
- i pazienti sospetti o accertati positivi al COVID-19 (di seguito Paziente), classificati come segue:
    1. paziente sospetto positivo in auto-isolamento o paziente accertato positivo in quarantena;
    2. paziente dimesso da ricovero ospedaliero. Possono inoltre essere sottoposti a monitoraggio preventivo, pazienti considerati ad alto rischio a causa delle condizioni di salute (es. cronici, immunodepressi, ecc.), che qualora contagiati sarebbero nelle condizioni di rischio vita.

Gli strumenti tecnologici, dettagliati puntualmente nel Capitolo 4, sono:

- una Piattaforma Applicativa per l'acquisizione dei dati clinici del Paziente;
- Kit di Telemonitoraggio composto dai seguenti costituito da vari componenti per la raccolta dei dati clinici del Pazienti;
- eventuale strumentazione per i MMG e per gli infermieri di studio (Case Manager), per l'utilizzo della Piattaforma Applicativa in mobilità.

Il **processo** si basa sul seguente modello di riferimento:

- per i pazienti in isolamento sospetti COVID-19 o COVID-19 positivi:
    - il MMG richiede alla Continuità Assistenziale l'attivazione del servizio per un Paziente;
    - la Continuità Assistenziale, in cooperazione con il MMG, prende contatto con il Paziente, richiede l'attivazione del servizio di telemonitoraggio e determina l'eventuale necessità anche un Kit di Telemonitoraggio nella sua composizione più idonea, lo assegna al Paziente, formandolo al suo utilizzo;
    - la Continuità Assistenziale, in cooperazione con il MMG, determina se attivare la Centrale Medica del Fornitore o di altro soggetto incaricato (ad es. Cooperativa MMG, …);
    - la Centrale Medica avvia il servizio di sorveglianza attiva contattando telefonicamente il paziente;
    - durante il periodo di telemonitoraggio i dati raccolti e gli allarmi generati dalla Piattaforma Applicativa sono messi a disposizione della Centrale Medica del Fornitore o di altro soggetto incaricato e resi visibili al MMG ed eventualmente all'erogatore ADI;
    - al termine del periodo di telemonitoraggio, il Paziente si reca all'ambulatorio per fare il tampone e restituisce il Kit di Telemonitoraggio;
    - il Centro Supporto Tecnologico preleva il Kit dall'ambulatorio per la sua sanificazione e la messa a disposizione per un prossimo Paziente.

- per i pazienti COVID positivi dimessi al domicilio:
    - alla dimissione del paziente, il Medico Ospedaliero determina l'eventuale necessità del Kit di Telemonitoraggio nella sua composizione più idonea e richiede alla Continuità Assistenziale l'attivazione del servizio per un Paziente;
    - la Continuità Assistenziale, prende contatto con il Paziente, prescrive l'attivazione del servizio di telemonitoraggio e ove richiesto assegna al Paziente il Kit di Telemonitoraggio nella sua composizione prevista, formandolo al suo utilizzo;
    - la Continuità Assistenziale, in cooperazione con il Medico Ospedaliero, determina se attivare la Centrale Medica del Fornitore o di altro soggetto incaricato (ad es. struttura ospedaliera, …);
    - la Centrale Medica avvia il servizio di sorveglianza attiva contattando telefonicamente il paziente;
    - durante il periodo di telemonitoraggio i dati raccolti e gli allarmi generati dalla Piattaforma Applicativa sono messi a disposizione della Centrale Medica del Fornitore o di altro soggetto incaricato e resi visibili al MMG, al Medico Ospedaliero ed eventualmente all'erogatore ADI;
    - al termine del periodo di telemonitoraggio, il Paziente si reca all'ambulatorio per fare il tampone e restituisce il Kit di Telemonitoraggio;
    - il Centro Supporto Tecnologico preleva il Kit dall'ambulatorio per la sua sanificazione e la messa a disposizione per un prossimo Paziente.

4. CARATTERISTICHE DELLA FORNITURA

Tutto quanto sopra premesso, si descrivono di seguito le caratteristiche del servizio, che il Fornitore dovrà mettere a disposizione.

4.1. Componenti Tecnologiche

4.1.1. Piattaforma Applicativa

La **Piattaforma** Applicativa consiste in una soluzione software, fruibile via Internet dai principali browser di mercato (Internet Explorer, Chrome, Firefox e Safari) e app mobili per i sistemi iOS e Android.

La Piattaforma Applicativa deve prevedere utenze profilate per l'utilizzo da parte del Paziente, MMG, Medico Ospedaliero, erogatore ADI e Centrale Medica del Fornitore o di altro soggetto incaricato.

La Piattaforma Applicativa deve poter essere fruibile, in tutte le sue funzionalità, da qualsiasi dispositivo connesso ad Internet (PC, tablet, smartphone, ecc.).

La Piattaforma Applicativa deve erogare le seguenti funzionalità:

- impostazione da parte del MMG e/o Medico Ospedaliero del piano di monitoraggio (tipologie, frequenza delle misurazioni da raccogliere e condizioni di allarme sui valori rilevati) su base singolo Paziente;
- impostazione da parte del MMG e/o Medico Ospedaliero del piano di sorveglianza attiva su base singolo Paziente;
- raccolta, secondo piano di monitoraggio e piano di sorveglianza definiti, dei dati clinici del Paziente raccolti in modalità automatica tramite integrazione con il Kit di Telemonitoraggio e/o in modalità manuale tramite inserimento in specifiche maschere di caricamento, da parte del Paziente e/o Caregiver e/o operatori della Centrale Medica, dei valori autonomamente rilevati;
- analisi dell'andamento dei dati clinici e segnalazione di allarmi al verificarsi delle condizioni definite;
- supporto alla Centrale Medica nella conduzione del monitoraggio e nella esecuzione della sorveglianza attiva secondo il Piano definito, attraverso la generazione automatica dell'elenco dei Pazienti da contattare, comprensivo anche di eventuali segnalazioni di attenzione inerenti al corretto svolgimento dell'attività di telemonitoraggio. L'elenco dovrà poter essere anche esportabile a terzi secondo un formato definito;
- tracciamento delle comunicazioni da e verso il Paziente con notifica delle comunicazioni intervenute al MMG/Medico Ospedaliero/operatore ADI;
- importazione di dati relativi al monitoraggio svolti da piattaforme applicative di altri Fornitori, secondo formati predefiniti;
- archiviazione su proprio repository dei dati trattati.

4.1.2. Kit di Telemonitoraggio

Il Kit di Telemonitoraggio consiste in:

- un terminale mobile (tablet o smartphone) dotato di connettività Internet tramite rete mobile;

- un insieme di dispositivi collegabili al terminale mobile tramite Bluetooth per la misura dei parametri di monitoraggio, costituito da:
    1. termometro per la misurazione della temperatura corporea;
    2. pulsossimetro per la misurazione della saturazione arteriosa di ossigeno e della frequenza cardiaca;
    3. dispositivo per misurazione della frequenza respiratoria;
    4. sfigmomanometro per la misurazione della pressione arteriosa;
    5. spirometro per la misurazione dei volumi polmonari.

La configurazione del Kit di Telemonitoraggio, in termini di quali dispositivi collegare al terminale mobile e la sua attivazione, dovranno poter essere svolte facilmente, autonomamente e con modalità semplificate da parte di personale non tecnico (ad esempio Medici e/o operatori di Continuità Assistenziale).

Al fine di garantire alla Stazione Appaltante l'approvvigionamento in tempi rapidi di dispositivi di misurazione, il Fornitore potrà proporre, in aggiunta a quanto sopra indicato, dispositivi di misurazione analoghi privi di connessione con terminale mobile, da utilizzarsi per la rilevazione manuale dei parametri.

I Kit di Telemonitoraggio dovranno essere messi a disposizione nei seguenti pacchetti:

- **Pacchetto A**: Terminale mobile + pulsossimetro;
- **Pacchetto B**: Terminale mobile + pulsossimetro + termometro;
- **Pacchetto C**: Terminale mobile + pulsossimetro + termometro + dispositivo per misurazione della frequenza respiratoria;
- **Pacchetto D**: Terminale mobile + pulsossimetro + termometro + sfigmomanometro;
- **Pacchetto E**: Terminale mobile + pulsossimetro + termometro + dispositivo per misurazione della frequenza respiratoria + sfigmomanometro;
- **Pacchetto F**: Terminale mobile + pulsossimetro + termometro + dispositivo per misurazione della frequenza respiratoria + sfigmomanometro + spirometro.

Il Fornitore potrà proporre per ogni pacchetto altri dispositivi di misura rispetto a quelli già complessivamente richiesti.

Il Fornitore dovrà altresì utilizzare, con modalità analoghe a quelle di sua Fornitura, anche eventuali dispositivi, tra quelli richiesti, messi a disposizione direttamente dalla Stazione Appaltante.

4.1.3. Strumentazione per MMG e infermieri di studio

La strumentazione per i MMG e infermieri di studio (Case Manager), consiste in un terminale mobile (tablet o smartphone) dotato di connettività Internet tramite rete mobile.

L'uso del terminale mobile è finalizzato a garantire l'operatività dei MMG e infermieri di studio (es. utilizzo della Piattaforma Applicativa per l'accesso ai parametri dei pazienti, video-consulti con Paziente e Caregiver), anche in mobilità.

4.1.4. Requisiti di certificazione

La Piattaforma Applicativa e i dispositivi di misurazione forniti dovranno essere certificati secondo la direttiva 93/42/CEE del 14/06/1993 concernente i dispositivi medici.

Dovranno essere, inoltre, in corso le attività di certificazione dei medesimi secondo il nuovo Regolamento Europeo dispositivi medici (MDR) 2017/745.

Al fine di consentire l'immediata attivazione del servizio, la certificazione delle integrazioni tra Piattaforma Applicativa e dispositivi medici, ove non già disponibile, potrà essere demandata ad un momento successivo all'attivazione del servizio. Il Fornitore dovrà, tuttavia, impegnarsi ad avviare da subito l'iter di certificazione con gli organismi competenti e a completarlo senza ingiustificati ritardi.

4.1.5. Interoperabilità e Requisiti non funzionali

Il repository della Piattaforma Applicativa dovrà consentire, anche successivamente all'attivazione ma su richiesta della Stazione Appaltante, la messa a disposizione di servizi di interoperabilità per connessione con i repository delle ATS lombarde erogati dalla Nuova Piattaforma Regionale d'Integrazione, consentendo la condivisione dei dati.

Più in generale la soluzione, anche successivamente all'attivazione, ma su richiesta della Stazione Appaltante, dovrà garantire i seguenti requisiti non funzionali:

- Coerenza con il contesto del SSR;
- Scalabilità, ovvero capacità della soluzione di distribuire la logica applicativa e i dati su più nodi fisici in caso di crescita degli utenti o picchi di utilizzo;
- Correttezza del dimensionamento del sistema;
- Affidabilità, ovvero capacità della soluzione di garantire un funzionamento continuativo e senza degradazioni delle prestazioni, non ultima la strategia di interscambiabilità con altre soluzioni di presa in carico del paziente già presenti sul territorio lombardo;
- Disponibilità, per ciascun utente abilitato, delle informazioni alle quali ha diritto di accedere, nei tempi e nei modi previsti anche in mobilità;
- Manutenibilità, ovvero garantire limitata complessità e oneri di manutenzione della soluzione erogata secondo il modello proposto, anche in relazione alle frequenti evoluzioni normative tipiche del contesto sanitario regionale lombardo o adattamento del profilo di presa in carico e di protocollo di cura;
- Semplificazione e standardizzazione dell'acceso ai servizi offerti dalla soluzione proposta;
- Integrità dei dati, ovvero la capacità di garantire sia l'integrità logica del dato in seguito a transazioni non andate a buon fine, sia l'integrità fisica del dato in caso di blocco del sistema;
- Sicurezza e rispetto della privacy, come descritto nel Capitolo 5;
- Conformità, ovvero aderenza allo standard di comunicazione HL7 e coerenza con i profili IHE (Integrating Healthcare Enterprise).

4.2. Centro Supporto Tecnologico

Il **Centro Supporto Tecnologico**, operante dalle 8.00 alle 20.00 7 giorni su 7, opera a supporto dei MMG, Medici Ospedalieri, Operatori CA, Centrale Medica, ed è incaricato di:

- erogare, gestire e manutenere la Piattaforma Applicativa esposta su Internet, con caratteristiche aderenti alle normative vigenti in materia di protezione dei dati personali/sicurezza delle informazioni;
- fornire e predisporre il Kit di Telemonitoraggio (terminale mobile e dispostivi) affinché possa essere configurato e attivato per l'uso sul Paziente con modalità semplificate da parte di operatori non tecnici;
- su base giornaliera, consegnare alla Continuità Assistenziale, nonché ritirare dagli ambulatori, i Kit di Telemonitoraggio rispettivamente all'avvio e al termine del loro utilizzo da parte del Paziente;
- provvedere alla sanificazione e manutenzione del Kit di Telemonitoraggio ritirato (comprensiva della completa cancellazione dei dati ivi registrati) prima del suo successivo riuso;
- fornire assistenza tecnica ai MMG, alla Continuità Assistenziale e alla Centrale Medica tramite Help Desk per l'utilizzo della Piattaforma Applicativa e del Kit di Telemonitoraggio.

4.3. Centrale Medica

La **Centrale Medica** del Fornitore, operante dalle 8.00 alle 20.00 7 giorni su 7, è incaricata, di:

- monitorare i dati e rilevare gli allarmi generati dalla Piattaforma Applicativa;
- svolgere sorveglianza attiva, tramite chiamate voce o con video, sui Pazienti secondo il piano di sorveglianza definito;
- gestire gli allarmi secondo i protocolli definiti (che possono prevedere il coinvolgimento del MMG e/o Medico Ospedaliero), tramite chiamate voce o con video;
- svolgere il ruolo di primo contatto per necessità dei Pazienti in collaborazione con il MMG e/o con la struttura che lo ha in carico, coinvolgendo il Centro Supporto Tecnologico nel caso di supporto inerente all'utilizzo della Piattaforma Applicativa e del Kit di Telemonitoraggio;
- raccogliere e registrare nella Piattaforma Applicativa le comunicazioni originate da e con i Pazienti e con il MMG di riferimento.

Il ruolo di Centrale Medica sarà erogato dal Fornitore, sulla base delle richieste provenienti dalla Continuità Assistenziale. Il ruolo potrà essere affidato anche ad altri operatori del Sistema Sanitario Regionale (es. Cooperative MMG, strutture ospedaliere, ADI, …), che utilizzeranno la Piattaforma Applicativa messa a disposizione dal Fornitore. Tale scelta si espliciterà in sede di richiesta di attivazione della tipologia di servizio per il singolo Paziente, così come descritto al Capitolo 6.

5. GESTIONE DELLA PRIVACY E DELLA SICUREZZA DELLE INFORMAZIONI

Di seguito vengono definiti i requisiti ai quali il Fornitore deve attenersi e/o implementare allo scopo di preservare l'integrità, la disponibilità e la riservatezza delle informazioni nell'ambito dell'erogazione della presente fornitura.

La sicurezza delle informazioni rappresenta un obiettivo di primaria importanza per ARIA. Al fine di consentire un'efficace ed efficiente gestione della sicurezza delle informazioni sotto tutti gli aspetti, il Fornitore si impegna a rispettare:

- Le prescrizioni normative in materia di protezione dei dati personali (D.Lgs. 196/03 successivamente rivisto con D.Lgs. 101/18, provvedimenti emanati dal Garante della Privacy);
- Quanto previsto dal Regolamento UE 2016/679 (Regolamento Europeo in materia di protezione dei dati personali, di seguito GDPR);
- Gli standard di settore, in particolare quelle richieste dalla ISO 27001/27002.

Il Fornitore si impegna a fornire tutto il supporto necessario per la risoluzione di eventuali incidenti o situazioni di crisi per la sicurezza delle informazioni in relazione all'oggetto del contratto. In particolare il Fornitore dovrà comunicare immediatamente a ARIA qualsiasi incidente occorso alle informazioni.

Tutto quanto definito e richiesto dal presente Allegato Tecnico in materia di gestione della sicurezza delle informazioni e privacy dovrà essere garantito dal Fornitore stesso e dai suoi eventuali sub fornitori.

5.1. Gestione della Privacy

Il D.Lgs. 196/03 successivamente rivisto con D.Lgs.101/18 e il Regolamento UE 2016/679 (Regolamento Europeo in materia di protezione dei dati personali, di seguito GDPR), nonché i Provvedimenti emanati dall'Autorità Garante per la Protezione dei dati personali (di seguito Garante Privacy), si prefiggono di garantire che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

Con "trattamento dei dati personali" s'intende nel seguito qualunque operazione (ad es.: consultazione, elaborazione, conservazione, ecc.) svolta con o senza l'ausilio di mezzi elettronici riguardante dati concernenti persone fisiche, giuridiche o enti.

Il D.Lgs. 196/03 successivamente rivisto con D.Lgs.101/18 stabilisce in particolare:

- La necessità di strutturare e mettere in atto un'organizzazione specifica per la Privacy attraverso l'identificazione di opportuni ruoli e le relative procedure di nomina;
- Un insieme di misure di sicurezza che devono essere applicate con lo scopo di assicurare un livello adeguato di protezione dei dati.

Il Garante Privacy ha inoltre espresso misure e accorgimenti specifici per i titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema (Provvedimento del 27 novembre 2008 e s.m.i.).

Nei paragrafi successivi vengono descritti, secondo l'ordine logico appena definito, i requisiti relativi alla normativa della privacy che il Fornitore dovrà rispettare.

5.1.1. Misure di sicurezza

L'articolo 5, par. 2 del Regolamento 679/2016/UE ("Principio di responsabilizzazione") impone che è responsabilità generale del titolare del trattamento per qualsiasi trattamento di dati personali mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare tale conformità delle attività di trattamento. Tali misure dovrebbero tenere conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche.

Quando il titolare del trattamento decide di affidarsi a soggetti esterni e questi, per poter svolgere l'attività, devono trattare dati personali di cui la titolarità è del titolare i soggetti esterni devono essere nominati quali responsabili del trattamento ex articolo 28 del Regolamento 679/2016/UE. Tale nomina a responsabile del trattamento impone che quest'ultimo svolga l'analisi dei rischi ex articolo 32 Regolamento 679/2016/UE anche sui trattamenti di dati personali svolti per conto del titolare del trattamento.

Il Fornitore verrà individuato quale responsabile del trattamento ex articolo 28 e riceverà dal titolare del trattamento la lettera di nomina contente tutte le indicazioni dell'articolo 28 del Regolamento 679/2016/UE.

Oltre all'applicazione delle misure di sicurezza, il trattamento dei dati personali, da parte del Fornitore, dovrà sempre ispirarsi al rispetto dei principi generali del D.Lgs. 196/03 successivamente rivisto con D.Lgs.101/18 e del GDPR e quindi avvenire in modo lecito e secondo correttezza, valutando la pertinenza, la completezza e la non eccedenza dei dati rispetto alle finalità dei trattamenti in funzione delle attività assegnate.

In particolare, si evidenzia il principio di minimizzazione (ex articolo 5, par. 1, lett. c del regolamento 679/2016/UE) che prevede che gli strumenti elettronici siano configurati in modo da ridurre al minimo l'utilizzo di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite possano essere realizzate mediante altri strumenti quali dati anonimi o altre modalità che permettano di identificare l'interessato solo in caso di necessità.

L'evoluzione della normativa sulla privacy, mediante la pubblicazione di provvedimenti, regolamenti, ecc. ad hoc da parte del Garante Privacy, ha richiesto e potrebbe richiedere in futuro, l'implementazione di misure di sicurezza specifiche. Si chiede quindi al Fornitore di considerare e applicare ogni ulteriore misura che potrà derivare dall'evoluzione normativa.

Inoltre, come previsto dal GDPR, deve essere adottato un approccio basato sulla *Security* e *Privacy by Design* e *by Default* che prevede l'adozione di adeguate misure di sicurezza a tutela di tutto il ciclo di vita del trattamento dei dati personali. Tali misure non sono definite puntualmente dalla normativa, ma devono essere selezionate dal Titolare e Responsabili attraverso opportune attività di analisi e verifica dei trattamenti e dei potenziali impatti in termini di privacy. Il Fornitore dovrà pertanto garantire il rispetto di tali misure e, al contempo, impegnarsi al rispetto delle misure di sicurezza identificate come necessarie ed opportune per il Servizio.

In particolare il Servizio:

- Tenendo conto dello stato dell'arte nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso, deve mettere in atto misure tecniche e organizzative adeguate volte ad attuare in modo efficace i principi di protezione dei dati, a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del Regolamento UE 2016/679 e tutelare i diritti degli interessati;
- Deve prevedere che la soluzione metta in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo deve valere per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In apposito registro dovranno essere tenuti aggiornati i referenti incaricati al trattamento e detto registro deve essere reso disponibile online dall'affidatario del servizio.

5.1.2. Provvedimento sugli Amministratori di Sistema

Il Garante Privacy ha stabilito specifiche misure di sicurezza e di verifica relativamente alle attività svolte da parte degli Amministratori di Sistema sui sistemi da loro gestiti.

Si rimanda al Provvedimento del Garante Privacy e s.m.i per la descrizione completa delle misure che il Fornitore è tenuto ad implementare nell'ambito oggetto del contratto. Di seguito si riportano i punti principali che il Fornitore è tenuto a rispettare:

- Identificare come Amministratori di Sistema le figure professionali finalizzate alla gestione ed alla manutenzione degli impianti di elaborazione e sue componenti e altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati personali;
- Attribuire le funzioni di Amministratore di Sistema previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza;
- Effettuare la designazione quale Amministratore di Sistema individualmente, allegando l'elenco analitico degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato;
- Riportare in un apposito documento, da mantenere aggiornato e disponibile ai diversi Titolari in caso di loro richiesta e al Garante Privacy in caso di accertamenti, gli estremi identificativi delle persone fisiche Amministratori di Sistema, con l'elenco delle funzioni ad essi attribuite. Detto registro deve essere consultabile dalle funzioni preposte dall'affidatario del servizio ed aggiornato on line a cura del fornitore;
- Adottare sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) da parte degli Amministratori di Sistema e degli utenti che accedono direttamente ai sistemi, ai database e alle console applicative dei sistemi, ai sistemi di virtualizzazione, dei dispositivi di rete, dei database ed alle applicazioni complesse. In particolare le registrazioni degli accessi devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro

integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate;

- Conservare le registrazioni degli accessi per un congruo periodo, non inferiore a sei mesi, rendendole accessibili alla consultazione da parte dei Titolari e degli organi giuridici che ne possono fare richiesta;
- Effettuare ogni 6 mesi (o in un periodo che potrà essere variato durante l'applicazione del contratto) una verifica delle attività svolte dagli Amministratori di Sistema, fornendo a tal fine evidenze a chi ha la titolarità delle banche dati e dei sistemi informatici.

Il Fornitore dovrà comunicare tempestivamente le nomine tramite apposita comunicazione a ARIA dove saranno inserite tutte le informazioni che garantiscono il rispetto degli aspetti richiesti dalla Normativa in vigore.

5.1.3. Data breach

Il Fornitore dovrà garantire la comunicazione al Titolare (ai sensi dell'art. 33.2 del Regolamento) di tutti gli eventi di violazione dei dati personali al fine di consentire al Titolare stesso il rispetto delle attività di notifica all'Autorità di controllo stabilite dall'articolo 33 del regolamento. La comunicazione da parte del Fornitore dovrà avvenire senza ingiustificato ritardo all'indirizzo PEC istituzionale e dovrà contenere almeno i seguenti punti:

- Natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- Il nome e i dati di contatto del Data Protection Officer o di altro punto di contatto presso cui ottenere più informazioni;
- Descrivere le probabili conseguenze della violazione dei dati personali;
- Descrivere le misure adottate da parte del responsabile del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Il responsabile sarà tenuto a mantenere presso i propri uffici la documentazione necessaria a descrivere le violazioni dei dati subite.

5.1.4. Cancellazione dei dati personali e sensibili

Si evidenzia che l'articolo 28 del Regolamento 679/2016/UE indica che il Fornitore deve cancellare e/o restituire al titolare tutti i dati personali una volta cessata l'erogazione dei servizi relativi al trattamento, cancellando anche le copie esistenti sui propri database, salvo che il diritto dell'Unione o degli stati membri preveda la conservazione dei dati; qualora al termine del servizio il titolare non richieda espressamente la restituzione dei dati questi si intenderanno soggetti ad obbligo di cancellazione.

5.1.5. Trasferimento e trattamento dei dati all'estero

Nel caso in cui, per l'erogazione del servizio si dovesse configurare la necessità di trasmettere dati personali degli interessati in Paesi al di fuori dell'Unione Europea, il Fornitore si impegna a

comunicare al titolare questo obbligo normativo, come imposto dall'articolo 28, par. 3, lett. a) del Regolamento 679/2016/UE, i Paesi nei quali i dati potranno essere comunicati al fine di poter idoneamente informare l'interessato. Al fine di rendere lecita la trasmissione il Titolare e il Fornitore concordano che le prescrizioni normative di riferimento sono quelle previste dagli articoli 44, 45, 46, 47, 48, 49, 50 del Regolamento 679/2016/UE; quindi qualora la trasmissione avvenisse in Paesi nei confronti dei quali non sussistessero decisioni di adeguatezza della Commissione Europea (ex. articolo 45 del Regolamento 679/2016/UE) e non sussistessero le garanzie adeguate di cui all'articolo 46 del Regolamento 679/2016/UE, il trasferimento potrà essere effettuato solamente sulla base di apposito consenso dell'interessato ai sensi dell'articolo 49, comma 1, lettera a) del Regolamento 679/2016/UE.

5.2. Gestione della sicurezza delle informazioni

5.2.1. Requisiti generali

Il Fornitore deve:

- Garantire il rispetto della normativa vigente (Leggi sul copyright, ecc.), anche attraverso l'implementazione di procedure appropriate;
- Garantire la riservatezza, l'integrità e la disponibilità delle informazioni gestite nell'ambito di tutte le attività ad esso affidate;
- Nell'ambito del trattamento, comunicazione e trasmissione di informazioni all'interno, così come verso l'esterno, rispettare il principio di:
    - Minimo privilegio;
    - Necessità;
    - Separazione dei compiti.
- Verificare con regolarità la conformità dei servizi erogati agli standard di sicurezza e ai requisiti richiesti da ARIA;
- Garantire la redazione di tutta la documentazione richiesta da ARIA in conformità agli standard definiti da ARIA;
- Raccogliere le evidenze, a seguito di un incidente di sicurezza, conservarle e presentarle qualora sussista la necessità di azioni legali di natura civile o penale;
- Impegnarsi formalmente a gestire in modo riservato e sotto la propria responsabilità le informazioni e i dati di cui viene a conoscenza. Al termine del contratto, salvo diverse disposizioni, le informazioni e i dati devono essere distrutti con modalità sicure o restituiti fornendo le relative evidenze a ARIA;
- Garantire che tutti gli strumenti di lavoro eventualmente introdotti in ARIA, come ad esempio laptop e dispositivi di memorizzazione, siano stati preventivamente autorizzati da ARIA e dotati di tutte le misure di sicurezza ritenute necessarie e adeguate (come nel caso dei gestori ed assistenti);

- Garantire che tutti gli strumenti di lavoro forniti da ARIA non siano modificati e la documentazione sia custodita con cura;
- Utilizzare sistemi antivirus, controllo malware e meccanismi di sicurezza per i media rimovibili, per tutte le postazioni e reti coinvolti nello svolgimento di attività per ARIA.

È vietata l'estrazione e il trasferimento di dati e/o di ogni altra informazione dalle basi dati e dai sistemi di ARIA, salvo espressa e preventiva autorizzazione da parte di ARIA.

5.2.2. Requisiti di sicurezza fisica

Il Fornitore, al fine di garantire a tutte le informazioni gestite per conto di ARIA adeguati livelli di tutela, deve definire, implementare e mantenere opportune soluzioni di sicurezza relativamente a: sicurezza perimetrale, controllo degli accessi fisici, sicurezza di uffici, locali tecnici ed attrezzature e quanto necessario: ad esempio l'alimentazione elettrica e la sicurezza dei cablaggi, i supporti di memorizzazione in ingresso e in uscita, lo smaltimento e il riutilizzo delle apparecchiature stesse. Nei prossimi paragrafi vengono illustrati i requisiti di sicurezza fisica che il Fornitore dovrà soddisfare in termini di: sicurezza delle postazioni di lavoro e delle reti e di infrastruttura del Fornitore.

Sicurezza delle postazioni di lavoro e delle reti

Il Fornitore, allo scopo di proteggere l'integrità, la disponibilità dei dati e di prevenire la divulgazione non autorizzata o l'utilizzo improprio delle informazioni, deve:

- Identificare e includere in qualunque tipo di accordo sui servizi di rete affidati all'esterno, le caratteristiche di sicurezza, i Livelli di servizio e i requisiti gestionali dei servizi di rete autorizzati;
- Garantire che i dati siano protetti contro il rischio di intrusione e dell'azione di software dannosi, mediante l'attivazione di idonei strumenti elettronici (es.: antivirus) curandone l'aggiornamento periodico.

Sicurezza dell'Infrastruttura del Fornitore

Il Fornitore, in funzione delle attività assegnate, deve implementare sulla propria infrastruttura e sulle proprie postazioni le opportune regole di sicurezza in funzione della criticità del servizio e/o dell'informazione trattata.

Nel dettaglio il Fornitore deve:

- Controllare e monitorare, tramite appostiti strumenti quali ad esempio firewall, IDS, i "punti di contatto" tra le reti interne del Fornitore e la rete di ARIA;
- Dotare le postazioni utilizzate dal Fornitore per accedere alla rete e ai sistemi di ARIA di opportuni meccanismi di sicurezza (antivirus, patch di sicurezza, etc);
- Prevedere con cadenza periodica, al fine di garantire efficienza e livelli di sicurezza adeguati alle postazioni e alle reti utilizzati:
    - Attività di hardening;
    - Attività di patching;

- Vulnerability/assessment/penetration test.

5.2.3. Requisiti di sicurezza organizzativa e logica

I requisiti di sicurezza organizzativa e logica che il Fornitore deve rispettare contribuiscono alla corretta gestione della sicurezza stessa all'interno dell'organizzazione, essendo finalizzati a prevenire ed impedire la perdita, il danneggiamento o il furto di beni/informazioni e l'interruzione dei servizi erogati. Nei prossimi paragrafi vengono illustrati i requisiti di sicurezza organizzativa e logica che il Fornitore dovrà soddisfare in termini di: requisiti per la firma digitale, requisiti di gestione delle risorse umane, requisiti di erogazione di servizi di fornitori terzi, controllo degli accessi e analisi e gestione dei rischi.

Requisiti per la firma digitale

Ove necessario il Sistema deve consentire la gestione di documenti (caricamento, conservazione, ….) in formato PDF firmati digitalmente (standard PAdES).

Il caricamento di ciascun documento, quando firmato digitalmente, deve essere condizionato all'esito positivo delle necessarie verifiche per l'accettabilità dello stesso (corrispondenza tra l'identità dell'utente loggato e quella del firmatario, validità del certificato utilizzato per la firma, …).

Requisiti di gestione delle risorse umane

Il Fornitore deve garantire che il proprio personale (Dipendenti, Collaboratori e fornitori terzi) coinvolto con i servizi oggetto della fornitura abbia piena consapevolezza delle problematiche relative alla sicurezza delle informazioni e applichi le norme di sicurezza.

Nel dettaglio il Fornitore per il personale coinvolto con la fornitura deve:

- Durante il proprio processo di ingaggio del personale, valutare i livelli di conoscenza degli obiettivi e delle problematiche di sicurezza in funzione delle attività che dovranno essere svolte;
- Prevedere un processo disciplinare formale relativo agli eventuali casi di violazione della sicurezza;
- Erogare un'adeguata e periodica formazione inerente le tematiche di sicurezza;
- Rimuovere, alla conclusione del rapporto di lavoro, tutti i diritti di accesso utilizzati per accedere alle reti, alle postazioni ed alle informazioni funzionali ai servizi oggetto della fornitura.

Requisiti di erogazione di servizi di fornitori terzi

Ove il Fornitore si avvalga di fornitori terzi per l'erogazione dei servizi oggetto della fornitura dovrà, come imposto dall'articolo 28, par. 2 e 4 del Regolamento 679/2016/UE, nominare tali fornitori terzi come sub-responsabili. Ai sensi dell'art.28.2 del Regolamento con la presente si fornisce espressa autorizzazione scritta generale alla individuazione da parte del Fornitore di altri soggetti che svolgano, per conto del Responsabile medesimo, il ruolo di "sub-responsabili". A fronte di tale autorizzazione, si richiede al Fornitore di comunicare alla scrivente l'elenco di tutti gli eventuali

soggetti individuati in qualità di sub-responsabili (fornitori terzi). La scrivente provvederà a verificare eventuali profili di criticità emergenti dalle comunicazioni ricevute e si riserva la facoltà di limitare e/o revocare l'autorizzazione ivi concessa. Nel caso in cui nel tempo intervengano modifiche, aggiunte o sostituzioni dei sub-responsabili inizialmente comunicati, tali nuove nomine dovranno essere inoltrate alla scrivente al fine di effettuare le opportune valutazioni (anche in termini oppositivi) relativamente alla protezione dei dati personali.

Si precisa come è obbligo del Responsabile del trattamento individuare e nominare in forma scritta i propri sub-responsabili; tale atto di nomina/individuazione dovrà riproporre a carico del sub-responsabile i medesimi obblighi posti a carico del responsabile e specificati nel presente documento, in particolare l'atto dovrà individuare le misure tecniche ed organizzative adeguate per garantire che il trattamento soddisfi i requisiti di sicurezza richiesti dal Regolamento.

Si evidenza come il Responsabile conservi nei confronti della scrivente, Titolare del trattamento, ogni responsabilità derivante dall'eventuale inadempimento posto in essere dal sub-responsabile.

Controllo degli accessi

Il Fornitore deve garantire sia sugli ambienti di ARIA sia sui propri che l'accesso alle informazioni, servizi e sistemi di ARIA avvenga in modo sicuro per prevenire l'accesso da parte di utenti che non hanno i necessari diritti e pertanto impedire trattamenti non autorizzati, tenuto conto che il ciclo di vita delle utenze è completamente in carico a ARIA

Nel caso di accesso ad ambienti di ARIA, il Fornitore deve:

- Richiedere in forma scritta la creazione di una nuova utenza che deve contenere l'identificativo della persona a cui verrà assegnata, l'ambito di utilizzo, il ruolo e l'ambiente. Le utenze richieste devono essere univoche, personali e utilizzate in modo che l'accesso alle informazioni da parte di ogni singolo utente sia limitato alle sole (principio del "minimo privilegio") informazioni di cui necessita (principio del "need-to-know") per lo svolgimento dei propri compiti;
- Inviare una tempestiva comunicazione a ARIA in caso di variazione delle mansioni o delle attività in modo che il profilo venga adeguato alle effettive nuove esigenze;
- Effettuare una revisione periodica delle utenze al fine di individuare le utenze inattive e quelle che necessitano di una modifica di privilegi da comunicare a ARIA;
- Richiedere immediatamente la disabilitazione di un'utenza assegnata ad un suo dipendente o collaboratore nei seguenti casi:
    - Interruzione del rapporto di lavoro con il Fornitore;
    - Cambio di mansione che non necessita dell'accesso ai servizi applicativi di ARIA;
    - Utenze inattive emerse nella revisione periodica.

L'accesso deve essere effettuato con autenticazione forte: smart card operatore oppure OTP.

Analisi e gestione dei rischi

Il Fornitore è tenuto a svolgere attività di analisi dei rischi rispetto alla sicurezza delle informazioni sull'intero oggetto del contratto.

In particolare l'analisi deve essere svolta almeno annualmente.

I risultati dell'analisi dei rischi devono essere presentati a ARIA dal Fornitore nei tempi e nei modi che saranno concordati opportunamente tra le parti e devono almeno prevedere:

- L'identificazione e la descrizione del rischio;
- Il livello di gravità del rischio;
- L'eventuale impatto sui servizi;
- Indicazioni sulle possibili soluzioni congiuntamente alle relative stime sui tempi e costi.

Il Fornitore, condividendolo con ARIA, definirà, ove necessario, le modalità di gestione del rischio (ovvero mitigazione, esternalizzazione ed accettazione) e sarà responsabile della redazione di un Piano di Trattamento dei Rischi da attuare nei tempi concordati con ARIA.

5.3. Verifica della conformità

5.3.1. Report da parte del Fornitore

Entro trenta giorni dalla stipula del contratto, il Fornitore dovrà predisporre una proposta di documento di autocertificazione periodica delle regole e delle policy relative alla sicurezza delle informazioni.

In particolare tale documentazione dovrà includere:

- La descrizione delle azioni implementate e delle regole definite;
- Il risultato dei test effettuati atti a garantire l'effettivo rispetto di tali regole.

Una volta approvato il documento da parte da ARIA, il Fornitore dovrà, mediante lo stesso, autocertificare annualmente o su richiesta di ARIA. Questa documentazione è considerata parte del sistema complessivo di monitoraggio della fornitura.

5.3.2. Attività di verifica e controllo

ARIA, avrà facoltà di effettuare o fare effettuare, eventualmente anche a terze parti, attività di verifica e controllo sull'applicazione, da parte del Fornitore ed eventualmente dei Subfornitori, di quanto sopra esposto e di qualsiasi altra misura di sicurezza che dovrà essere implementata a fronte di nuove politiche definite da ARIA. La verifica può essere effettuata sia tramite visita presso il Fornitore o congiuntamente presso il suo SubFornitore, sia tramite richiesta di idonea documentazione attestante la conformità alla normativa.

A fronte di difformità rilevate, il Fornitore si impegna ad eseguire gli interventi per il superamento delle stesse previa validazione da parte di ARIA delle soluzioni identificate.

6. DIMENSIONAMENTO DEL SERVIZIO E PIANO DEI CORRISPETTIVI

6.1. Dimensionamento del servizio

Si riportano di seguito le informazioni stimate inerenti al dimensionamento del servizio. Si precisa che tutte le informazioni fornite sono da considerarsi indicative e non vincolanti per la Stazione Appaltante, sia in termini di numero di Pazienti assegnati che di composizione delle tipologie di modalità di servizio o pacchetti richiesti.

Al Fornitore sarà affidata l'erogazione del servizio sui pazienti di una o più aree territoriali (Lotti). I pazienti sono distribuiti sulle aree sulla base delle informazioni oggi a disposizione, come di seguito indicato:

- **Lotto 1**: ATS Città Metropolitana di Milano;
- **Lotto 2**: ATS Bergamo;
- **Lotto 3**: ATS Brescia, ATS Montagna;
- **Lotto 4**: ATS Val Padana, ATS Pavia, ATS Brianza, ATS Insubria.

Il Fornitore è chiamato ad erogare il servizio, sulla base delle richieste della Continuità Assistenziale, secondo le seguenti modalità:

- **Modalità 1**: Fornitura della Piattaforma Applicativa (da applicare agli erogatori del servizio che non dispongono di una piattaforma propria);
- **Modalità 2**: Servizio di telemonitoraggio base (Piattaforma Applicativa e Servizi della Centrale Medica del Fornitore)
- **Modalità 3**: Servizio di telemonitoraggio avanzata senza Centrale Medica (Piattaforma Applicativa, Kit di Telemonitoraggio)
- **Modalità 4**: Servizio di telemonitoraggio avanzato con Centrale Medica (Piattaforma Applicativa, servizi della Centrale Medica del Fornitore e Kit di Telemonitoraggio)

Nelle modalità 1 e 3 il ruolo di Centrale Medica sarà svolto da strutture ospedaliere e cooperative MMG accreditate per la presa in carico dei pazienti attraverso l'utilizzo dei rimanenti servizi del Fornitore (es. Piattaforma Applicativa e Kit di Telemonitoraggio, ove previsto).

Si ipotizza che i Pazienti su cui erogare i servizi in questione siano ripartiti, sui diversi scenari descritti come segue:

- Modalità 1: 10 %;
- Modalità 2: 40 %;
- Modalità 3: 10 %;
- Modalità 4: 40 %.

In relazione ai pacchetti dei Kit di Telemonitoraggio descritti al paragrafo 4.1.2, la loro distribuzione sui pazienti si ipotizza così costituita:

- **Pacchetto A**: Terminale mobile + pulsossimetro: 40%;
- **Pacchetto B**: Terminale mobile + pulsossimetro + termometro: 30%;
- **Pacchetto C**: Terminale mobile + pulsossimetro + termometro + dispositivo per misurazione della frequenza respiratoria: 15%;
- **Pacchetto D**: Terminale mobile + pulsossimetro + termometro + sfigmomanometro: 10%;

- **Pacchetto E**: Terminale mobile + pulsossimetro + termometro + dispositivo per misurazione della frequenza respiratoria + sfigmomanometro: 4%;
- **Pacchetto F**: Terminale mobile + pulsossimetro + termometro + dispositivo per misurazione della frequenza respiratoria + sfigmomanometro + spirometro: 1%.

Nel caso di impossibilità del Fornitore di mettere a disposizione il pacchetto di Kit di Telemonitoraggio richiesto nei tempi previsti, il servizio dovrà essere comunque erogato tramite *downgrade* al primo pacchetto di categoria inferiore disponibile o, in estrema ratio, al servizio da modalità 1 o 2, qualora la richiesta originaria fosse, rispettivamente, per la modalità 3 o 4.

Si considera applicato il *downgrade* qualora non venga fornito il pacchetto richiesto entro 12 ore lavorative dalla richiesta.

6.2. Listini

Nella configurazione di servizio e secondo le ipotesi sopra esposte, la composizione del costo del servizio da affidare ai Fornitori sarà organizzata come segue:

	Servizi di telemonitoraggio	**Importo (IVA esclusa)**
Costo a consumo per paziente (per 14 giorni di utilizzo)	Modalità 1	20 €
	Modalità 2	150€
	Modalità 3	Fino a 140 € (a seconda del pacchetto di dispositivi utilizzato)
	Modalità 4	130 € + fino a 140 € (a seconda del pacchetto di dispositivi utilizzato)

I costi riconosciuti nelle modalità 3 e 4 varieranno in funzione del pacchetto di dispositivi utilizzato.

La tabella seguente riporta i relativi listini distinguendo tra dispositivi integrati (ovvero connessi tramite bluetooth) e dispositivi non integrati (ovvero non connessi) con il terminale mobile.

	Kit di Telemonitoraggio	**Importo (IVA esclusa)**	
		Integrati	**Non integrati**
Costo a consumo per paziente (per 14 giorni di utilizzo)	**Pacchetto A**	60 €	15 €
	Pacchetto B	78 €	20 €
	Pacchetto C	100 €	25€
	Pacchetto D	100 €	25 €
	Pacchetto E	121 €	30 €

	Pacchetto F	140 €	35 €

In caso di erogazione in *downgrade*, il costo riconosciuto sarà calcolato applicando una riduzione del 20% al costo totale della modalità effettivamente erogata (ovvero comprensiva di eventuale importo base e importo in funzione del pacchetto effettivamente fornito).

La Tabella seguente riporta il listino relativo alla Dotazione di strumentazione in mobilità a medici e infermieri.

	Dotazione di strumentazione in mobilità a medici e infermieri	**Importo (IVA esclusa)**
Costo una tantum a dispositivo	Dispositivo mobile	400 €

6.3. Durata e valore massimo stimato

La Durata del contratto è pari a 6 (sei) mesi.

Il Valore massimo stimato per ogni Lotto è pari a 1.066.000,00 € (IVA esclusa).

Il Valore massimo stimato non sarà soggetto a ribasso. Gli sconti offerti dai concorrenti saranno applicati ai prezzi unitari.

La Stazione Appaltante si riserva la facoltà di richiedere di incrementare, alle stesse condizioni, la fornitura fino a concorrenza del limite di un quinto dell'importo complessivo aggiudicato, al netto di Iva e/o di altre imposte e contributi di legge, nonché degli oneri per la sicurezza dovuti a rischi da interferenze, e fino al raggiungimento del medesimo.

7. LIVELLI DI SERVIZIO

Il capitolo definisce gli indicatori atti a descrivere i Livelli di Servizio (LdS), che verranno applicati, le relative modalità di rilevazione, i LdS minimi richiesti e il periodo di riferimento su cui calcolare il valore dell'indicatore.

Il Fornitore è tenuto a produrre e consegnare i rapporti di dettaglio che verranno utilizzati per la valutazione del rispetto dei Livelli di Servizio costruiti secondo formati e contenuti coerenti con la tipologia dell'indicatore in esame e con periodicità congruente con il relativo periodo di riferimento.

I rapporti dovranno essere prodotti per tutti i Livelli di Servizio riportati nel presente capitolo, fatto salvo ove espressamente indicato. Per alcuni Livelli di Servizio, esplicitamente indicati, le informazioni elementari raccolte dal Fornitore per il calcolo degli stessi dovranno essere registrate, su base giornaliera, in specifici file in formato.csv, che dovranno:

- possedere un identificativo progressivo;
- essere marcati temporalmente.

Si precisa che tali file dovranno essere prodotti secondo uno schema condiviso e approvato con ARIA e inviati su base mensile e che potranno essere utilizzati per verificare la correttezza dei rapporti dei Livelli di Servizio.

Indipendentemente dal periodo di riferimento (variabile in relazione allo specifico indicatore) il Fornitore è tenuto ad uno stretto controllo dell'andamento dei livelli qualitativi dei servizi offerti per intervenire tempestivamente nel ripristino dei valori obiettivo non appena si rilevino deviazioni significative. Il non rispetto dei Livelli di Servizio in seguito alla rilevazione del superamento dei valori di soglia crea le condizioni per azioni contrattuali.

La definizione dei Livelli di Servizio riportati nei paragrafi che seguono è rappresentata attraverso il seguente prospetto:

Codifica del LdS	**Acronimo del servizio – LdSxx(n° progressivo per linea di servizio)** es.SD-LdS03 *(per Service Desk - Livello di Servizio n°03)*
Titolo del LdS	**Indicazione sintetica del Livello di Servizio** *(es. "Presa in carico di segnalazioni a priorità media")*
Descrizione del LdS	Descrizione di ciò che il LdS si prefigge di misurare (obiettivo del LdS)
Unità di misura	Descrizione dell'unità di misura utilizzata per quantificare il LdS
Periodo di riferimento	Periodo temporale di riferimento per il calcolo dell'indicatore
Frequenza di misurazione	Periodicità della misurazione
Dati da rilevare	Definisce le misure elementari da rilevare per il calcolo del LdS
Formula	Descrizione della modalità di calcolo (formula e misure)
Valore di soglia (Risultati attesi)	Definisce le soglie di riferimento per le valutazioni delle performance di servizio ed il rispetto dei livelli contrattuali. È possibile definire più soglie in funzione di diversi livelli di prestazione previsti
Sanzione	Indicazione della tipologia di sanzione attivata dall'occasionale e/o reiterato mancato rispetto del LdS

Note	Eventuali annotazioni a margine relative a esclusioni, casi particolari, ecc. che influenzino il calcolo, la validità o altri elementi dello SLA.

I Livelli di Servizio saranno misurati su base solare o nell'orario lavorativo **dalle 8.00 alle 20.00, 7 giorni su 7**, così come specificatamente indicato.

I fermi programmati e gli interventi di manutenzione straordinaria non influiscono nel calcolo dei Livelli di Servizio più oltre definiti e dovranno essere effettuati, possibilmente nella fascia oraria notturna, previa comunicazione scritta a ARIA da inviare con un anticipo di almeno cinque (5) giorni lavorativi.

Tutte le interruzioni del servizio che non rientrano nella casistica sopra delineata sono considerate indisponibilità del servizio e incidono nel calcolo dei Livelli di Servizio.

Codifica del LdS	**LdS01**
Titolo del LdS	**Disponibilità della Piattaforma**
Descrizione del LdS	Misura della disponibilità della Piattaforma Applicativa.
Unità di misura	Percentuale.
Periodo di riferimento	Settimana solare precedente la rilevazione.
Frequenza di misurazione	Settimanale.
Dati da rilevare	Tr_i = tempo di indisponibilità espresso in ore solari causato dal i-esimo malfunzionamento. Td = tempo di disponibilità prevista nel periodo di riferimento espresso in ore solari. N = numero di malfunzionamenti.
Formula	$LdS = \frac{Td - \sum_{i=1}^{N} Tr_i}{Td}$ (trasformato in %, ad es. 0,964 corrisponde al 96,4%)
Valore di soglia	$LdS \geq 99{,}99\%$
Tipo Sanzione	Applicazione di una penale pari allo 0,3 ‰ dell'ammontare netto contrattuale al primo scostamento al di sotto della soglia e per ogni scostamento pari a 0,01% fino ad un massimo di 5 scostamenti.
Note	

Codifica del LdS	**LdS02**
Titolo del LdS	**Attivazione del Paziente sulla Piattaforma**
Descrizione del LdS	Misura del tempo di attivazione del Paziente sulla Piattaforma Applicativa.
Unità di misura	Ore lavorative.
Periodo di riferimento	Giorno lavorativo precedente la rilevazione.
Frequenza di misurazione	Giornaliera.

Dati da rilevare	N = numero di Pazienti attivati nel periodo di riferimento. Tri = tempo di attivazione del i-esimo Paziente espresso in ore lavorative a partire dalla richiesta di attivazione proveniente dalla Continuità Assistenziale.
Formula	LdS = $\frac{\sum_{i=1}^{N} \mathrm{Tr}_i}{N}$
Valore di soglia	LdS ≤ 1 ora lavorativa
Tipo Sanzione	Applicazione di una penale pari allo 0,3 ‰ dell'ammontare netto contrattuale al primo scostamento al di sopra della soglia e per ogni scostamento pari a 1 ora lavorativa fino ad un massimo di 5 scostamenti.
Note	Oggetto di registrazione giornaliera dei dati elementari necessari al calcolo del Livello di Servizio.

Codifica del LdS	**LdS03**
Titolo del LdS	**Tempo di indisponibilità del Kit di Telemonitoraggio presso la Continuità Assistenziale**
Descrizione del LdS	Misura il tempo in cui la Continuità Assistenziale rimane priva di Kit di Telemonitoraggio da consegnare ai Pazienti.
Unità di misura	Ore lavorative.
Periodo di riferimento	Giorno lavorativo precedente la rilevazione.
Frequenza di misurazione	Giornaliera.
Dati da rilevare	N = numero di richieste di telemonitoraggio di Pazienti che richiedono l'attivazione del Kit. Ti = tempo di indisponibilità del Kit di Telemonitoraggio registrato per la gestione della i-esima richiesta di attivazione.
Formula	LdS = $\sum_{i=1}^{N} \mathrm{Ti}_i$
Valore di soglia	LdS ≤ 4 ore lavorative
Tipo Sanzione	Applicazione di una penale pari allo 0,3 ‰ dell'ammontare netto contrattuale al primo scostamento al di sopra della soglia e per ogni scostamento pari a 1 ora lavorativa fino ad un massimo di 5 scostamenti.
Note	Oggetto di registrazione giornaliera dei dati elementari necessari al calcolo del Livello di Servizio.

Codifica del LdS	**LdS04**
Titolo del LdS	**Tempo di risposta Centro Supporto Tecnologico**
Descrizione del LdS	Misura il tempo richiesto per la risposta da parte del Centro Supporto Tecnologico a richieste di assistenza.
Unità di misura	Minuti lavorativi.
Periodo di riferimento	Giorno lavorativo precedente la rilevazione.
Frequenza di misurazione	Giornaliera.

Dati da rilevare	N = numero di richieste di assistenza ricevute nel periodo di riferimento. Tr_i = tempo di risposta alla richiesta di assistenza.
Formula	$LdS = \frac{\sum_{i=1}^{N} Tr_i}{N}$
Valore di soglia	LdS ≤ 5 minuti lavorativi
Tipo Sanzione	Applicazione di una penale pari allo 0,3 ‰ dell'ammontare netto contrattuale al primo scostamento al di sopra della soglia e per ogni scostamento pari a 1 minuto lavorativo fino ad un massimo di 5 scostamenti.
Note	Oggetto di registrazione giornaliera dei dati elementari necessari al calcolo del Livello di Servizio.

Codifica del LdS	**LdS05**
Titolo del LdS	**Rispetto dei Piani di Sorveglianza**
Descrizione del LdS	Misura il rispetto nella esecuzione delle chiamate di sorveglianza al Paziente all'interno delle fasce temporali indicati nel Piando di Sorveglianza.
Unità di misura	Ore lavorativa.
Periodo di riferimento	Giorno lavorativo precedente la rilevazione.
Frequenza di misurazione	Giornaliera.
Dati da rilevare	Tr = scostamento temporale della singola chiamata rispetto alla fascia temporale pianificata.
Formula	LdS = Tr
Valore di soglia	LdS ≤ 1 ora lavorativa
Tipo Sanzione	Applicazione di una penale pari allo 0,3 ‰ dell'ammontare netto contrattuale al primo scostamento al di sopra della soglia e per ogni scostamento pari a 1 ora lavorativa.
Note	Oggetto di registrazione giornaliera dei dati elementari necessari al calcolo del Livello di Servizio.

Codifica del LdS	**LdS06**
Titolo del LdS	**Tempo di risposta Centrale Medica**
Descrizione del LdS	Misura il tempo richiesto per la risposta da parte della Centrale Medica a chiamate di Pazienti.
Unità di misura	Minuti lavorativi.
Periodo di riferimento	Giorno lavorativo precedente la rilevazione.
Frequenza di misurazione	Giornaliera.
Dati da rilevare	N = numero di chiamate ricevute nel periodo di riferimento. Tr_i = tempo di risposta alla chiamata.
Formula	$LdS = \frac{\sum_{i=1}^{N} Tr_i}{N}$

Valore di soglia	LdS ≤ 5 minuti lavorativi
Tipo Sanzione	Applicazione di una penale pari allo 0,3 ‰ dell'ammontare netto contrattuale al primo scostamento al di sopra della soglia e per ogni scostamento pari a 1 minuto lavorativo fino ad un massimo di 5 scostamenti.
Note	Oggetto di registrazione giornaliera dei dati elementari necessari al calcolo del Livello di Servizio.

Codifica del LdS	**LdS07**
Titolo del LdS	**Tempo di risoluzione delle richieste di assistenza**
Descrizione del LdS	Rispetto del tempo di risoluzione delle richieste di assistenza da parte del Centro Supporto Tecnologico.
Unità di misura	Percentuale
Periodo di riferimento	Giorno lavorativo precedente la rilevazione.
Frequenza di misurazione	Giornaliera
Dati da rilevare	NcOK = numero di ticket chiusi nella tempistica previste nel periodo di riferimento. NcT = numero di ticket chiusi nel periodo di riferimento.
Formula	LdS = $\frac{\text{NcOK}}{\text{NcT}}$ (trasformato in %, ad es. 0,855 corrisponde a 85,5%)
Valore di soglia	LdS ≥ 90,00% Tempistica previste per la chiusura dei ticket: 4 ore lavorative.
Tipo Sanzione	Applicazione di una penale pari allo 0,3 ‰ dell'ammontare netto contrattuale al primo scostamento al di sotto della soglia e per ogni scostamento pari a 2% fino ad un massimo di 5 scostamenti.
Note	Oggetto di registrazione giornaliera dei dati elementari necessari al calcolo del Livello di Servizio.

Codifica del LdS	**LdS08**
Titolo del LdS	**Produzione dei rapporti di dettaglio dei Livelli di Servizio erogati**
Descrizione del LdS	Misura il tempo intercorrente tra la consegna del rapporto di dettaglio la cui produzione è in capo al Fornitore e il termine del relativo periodo di riferimento.
Unità di misura	Giorni lavorativo.
Periodo di riferimento	Settimana lavorativo precedente la rilevazione.
Frequenza di misurazione	Settimanale.

Dati da rilevare	N = numero di rapporti previsti nel periodo di riferimento. Tr_i = tempo dalla data di termine del periodo di riferimento del rapporto i-esimo e la sua data di consegna da parte del Fornitore.
Formula	LdS = $\frac{\sum_{i=1}^{N} Tr_i}{N}$
Valore di soglia	LdS ≤ 1 giorno lavorativo
Tipo Sanzione	Applicazione di una penale pari allo 0,3 ‰ dell'ammontare netto contrattuale al primo scostamento al di sopra della soglia e per ogni scostamento pari a 1 giorno solare.
Note	