REGIONE PUGLIA

CAPITOLATO TECNICO di
Appalto specifico

AFFIDAMENTO DI «SERVIZI APPLICATIVI E DI SERVIZI ACCESSORI IN AMBITO DI CARTELLA CLINICA ED ENTERPRISE IMAGING» MEDIANTE APPALTO SPECIFICO NELL'AMBITO DELL'ACCORDO QUADRO «SANITA' DIGITALE - Sistemi Informativi Clinico-Assistenziali 2» PER LE PUBBLICHE AMMINISTRAZIONI DEL SSN

ID 2601 Lotto 2: Cartella Clinica Elettronica CENTRO - SUD

INDICE

1 Indice

1 ELEMENTI GENERALI

Il presente Appalto Specifico rientra nell'ambito dell'Accordo Quadro del Lotto 2: Cartella Clinica Elettronica– CENTRO - SUD

Fanno parte integrante del predetto Capitolato Tecnico le seguenti appendici:

- Appendice 1 Profili Professionali
- Appendice 2 Livelli di Servizio
- Appendice 3 Cicli e Prodotti
- Appendice 4 CCE - Analisi dei processi
- Appendice 5 CCE - Specifiche di architettura
- Appendice 6 CCE - SRS Cartella Clinica

Le indicazioni contenute nel presente Capitolato Tecnico e relative appendici rappresentano i requisiti minimi dell'Appalto Specifico (aggiuntivi ai requisiti già espressi nel Capitolato Tecnico dell'Accordo Quadro e delle Offerte Tecniche integrative) che devono essere soddisfatti per l'affidamento dei servizi.

Il Capitolato Tecnico dell'Accordo Quadro e le relative appendici costituiscono parte integrante della presente iniziativa, ancorché non materialmente allegati.

Definizioni

Nel corpo del presente Capitolato Tecnico, con il termine:

- ADT: Accettazione Dismissione Trasferimento
- AgID: Agenzia per Italia Digitale
- AO: Azienda Ospedaliera
- API: Application Programming Interface
- AQ: Accordo Quadro
- AS: si intende il presente Appalto Specifico
- ASL: Azienda Sanitaria Locale
- CAD: Codice dell'Amministrazione Digitale
- CDR: Clinical Data Repository
- CEDAP: Certificato di Assistenza di Parto
- CONSIP: Consip S.p.A.
- COT: Centrale Operativa Territoriale
- CT: Capitolato Tecnico
- CTS: Capitolato Tecnico Specifico
- CUP: Centro Unico di Prenotazione
- DEA: Dipartimento di Emergenza e Accettazione
- FHIR: Fast Healthcare Interoperability Resources
- FSE: Fascicolo Sanitario Elettronico
- FUT: Foglio Unico di Terapia
- GDPR: General Data Protection Regulation - Regolamento generale sulla protezione dei dati
- HL7: Health Level Seven
- HTTP: Hyper Text Transport Protocol
- HTTPS: Hyper Text Transport Protocol Secure
- IaaS: Infrastructure as a Service
- ICT: Information and Communication Technology
- IHE: Integrating the Healthcare Enterprise
- ISO: International Organization for Standardization
- IVG: Interruzione Volontaria di Gravidanza
- LIS: Laboratory Information System

- PaaS: Platform as a Service
- PDTA: Percorsi Diagnostico Terapeutici Assistenziali
- PNRR: Piano Nazionale di Ripresa e Resilienza
- PT: Penetration Test
- RIPO: Registro Regionale di Implantologia Protesica
- SaaS: Software as a Service
- SAL: Stato Avanzamento Lavori
- SI: Sistema Informativo
- SPID: Sistema pubblico di identità digitale
- SSR: Sistema Sanitario Regionale
- VA: Vulnerability Assessment
- WAS: Web Application Scan
- XML: eXtensible Markup Language

2 CONTESTO DELL'APPALTO SPECIFICO

La presente iniziativa si colloca nel contesto di attuazione, da parte di Regione Puglia (di seguito anche "Amministraziore") del "Piano di Sanità Digitale della Regione Puglia per il triennio 2018/2020" approvato dalla Giunta Regionale con deliberazione n. 1803/2019 e del successivo Piano Triennale di Riorganizzazione Digitale 2022-2024 e relativo aggiornamento 2023-2025 approvati rispettivamente con con Deliberazione Della Giunta Regionale n. 30 maggio 2022, n. 791 e n. 1094 del 31 luglio 2023 e riguarda l'intervento denominato "Realizzazione della Cartella Clinica Elettronica del Servizio Sanitario Regionale Pugliese.". Tale intervento, a valere sulle risorse FSC 2014/2020, è stato approvato con Deliberazione di Giunta Regionale n. 1850 del 14/10/2019.

Gli interventi previsti all'interno della presente iniziativa rivestono particolare importanza permettendo di procedere al completamento della digitalizzazione e dematerializzazione dei processi, con particolare riferimento al percorso di ricovero ed ambulatoriale dei pazienti con l' evoluzione di una Cartella Clinica Elettronica di ricovero e ambulatoriale evoluta, in grado di coprire tutti gli ambiti operativi e funzionali garantendo la collaborazione clinica e la condivisione dei dati, di una Cartella di Pronto Soccorso per l'accettazione, gestione e trattamento dei pazienti che accedono in regime di emergenza/urgenza, nonché l'introduzione di alcune altre componenti applicative come successivamente indicato.

Contesto tecnologico ed applicativo

La Regione Puglia, negli ultimi anni, ha avviato un percorso di ammodernamento del Sistema Sanitario Regionale, con particolare attenzione allo sviluppo della Sanità digitale, che l'ha resa in breve tempo una tra le Regioni più proattive e innovative. In particolare, l'esigenza espressa dalla Regione Puglia, successivamente tradotta nella realizzazione della Cartella Clinica Elettronica (CCE), è stata quella di uniformare i percorsi clinici e ambulatoriali attraverso una soluzione unica in grado di fornire un supporto alla gestione informatizzata dei dati anagrafici, clinici e sanitari del paziente, lungo tutto il ciclo di assistenza. In questo modo si è fornito un accesso istantaneo alle informazioni sanitarie, mettendo a disposizione del personale sanitario dei validi strumenti di supporto per la gestione del paziente, permettendo così di strutturare percorsi di cura partecipati e condotti in un rapporto medico paziente sempre più integrato.
Il sistema integrato attuale di sanità digitale è attualmente composto, a titolo esemplificativo e non esaustivo, oltre che dal Sistema Informativo di Cartella Clinica Elettronica regionale, anche dalle seguenti strutture digitali e tecnologiche:

- Il Sistema Edotto, mediante il quale oggi si governano i servizi di base della Sanità, come l'assistenza primaria, i processi assistenziali, l'accesso al pronto soccorso, l'accettazione dei ricoveri ospedalieri, la distribuzione diretta di farmaci, la presa in carico domiciliare e la presa in carico residenziale;

- Il Sistema Informativo Sanitario Territoriale (SIST), per la gestione delle prescrizioni elettroniche e dematerializzate, volto ad assicurare la continuità delle cure tra ospedale e territorio, tramite il collegamento con medici di famiglia, farmacie, specialisti ambulatoriali e ospedalieri, pronto soccorso, laboratori di analisi e il Fascicolo Sanitario Elettronico (FSE);
- Il Portale della Salute, punto unico di accesso per i cittadini ai servizi digitali regionali, racchiude al suo interno i siti istituzionali delle dieci Aziende pubbliche e degli Organismi ed Enti del Servizio Sanitario Regionale con un'organizzazione federata. Sul portale e sull'applicazione PugliaSalute è possibile usufruire di servizi informativi e interattivi quali: prenotazione e disdetta di una visita o un esame, pagamento di ticket, scelta del medico e del pediatra, informazioni sulle proprie esenzioni, gestioni dei buoni per celiaci, diario delle vaccinazioni, scaricare i propri referti online dal FSE;
- Il CUP federato per ampliare le prestazioni dei singoli CUP aziendali secondo un principio di contiguità territoriale, sull'intera area regionale;
- Il Servizio di Emergenza-Urgenza Sanitaria Territoriale 118, che è uno dei sistemi più evoluti tecnologicamente sul piano nazionale e permette la gestione in tempo reale delle cinque Centrali Operative 118, dei mezzi mobili di soccorso e dell'emergenza/urgenza sull'intero territorio regionale;
- Il SIRDImm che rappresenta un'unica soluzione software per la gestione dei servizi di diagnostica per immagini erogati dalle aziende sanitarie pubbliche della Regione consentendo il completo passaggio al digitale di dati e documenti relativi alla diagnostica per immagini tramite anche opportune integrazioni con i sistemi informativi aziendali e regionali;
- SISM/Dipendenze Patologiche che soddisfano le necessità degli operatori territoriali dei Dipartimenti di Salute Mentale e delle Dipendenze Patologiche;
- Sistema Informativo regionale Trasfusionale per la gestione a livello regionale degli emocomponenti, delle trasfusioni, dei donatori di sangue;
- Il Sistema Informativo regionale per la rete Parkinson per gestire la presa in carico dei pazienti affetti dalla malattia in modo uniforme e condiviso.

Il sistema integrato di Sanità digitale comprende inoltre altri sistemi regionali, quali:

- GIAVA, per l'informatizzazione degli ambulatori e delle procedure vaccinali;
- Sistema Informativo Regionale di Anatomia Patologica per la gestione delle attività svolte presso gli 11 Servizi di Anatomia Patologica della Regione Puglia, in linea con quanto previsto dalla DGR DR 1335/2018 di istituzione della rete delle anatomie patologiche della Puglia, al fine di garantire la tracciabilità del campione dal momento del prelievo e durante il ciclo lavorativo, sino alla fase di refertazione e conferimento del referto ai soggetti richiedenti;
- Sistema per gli Screening Oncologici per la gestione dei processi di screening della Cervice uterina, della Mammella e del Colon Retto;
- Sistema Informativo Regionale per la Medicina dello sport: per la gestione della procedura per il rilascio del certificato di idoneità per la pratica sportiva agonistica;
- Sistema Informativo IRIS "Infection Regional Information System", dedicato alla gestione delle malattie infettive e delle connesse attività di sorveglianza epidemiologica.

Sistema Informativo	**Fornitore**
CCE - Cartella Clinica Elettronica ricovero e ambulatoriale	Exprivia S.p.A/Enterprice Services Italia s.r.l.
Pronto Soccorso - Edotto Build	Exprivia S.p.A.
SIST - Sistema Informativo Sanitario Territoriale	Deda Next Srl
Portale della Salute PugliaSalute	RTI Enterprise Services Italia s.r.l., Exprivia Spa e DGS spa
e-CUP - CUP federato	Soluzione in riuso

Servizio di emergenza-urgenza sanitaria territoriale 118	ISED
SIRDIMM – Sistema Informativo regionale per la diagnostica per immagini	AGFA Gevaert S.p.A.
SISM – Sistema Informativo regionale dei Dipartimenti della Salute Mentale	Exprivia S.p.A.
SIRDIP - Sistema Informativo regionale per le Dipendenze Patolgiche	Exprivia S.p.A.
SIRT – Sistema Informativo regionale Trasfusionale	Almaviva S.p.A.
Sistema Informativo Rete Parkinson	CLE S.r.l., GPI S.p.A.
SIRAP - Anatomia patologica	Enterprise Services Italia S.r.l. (A DXC Technology Company) - P.IVA Subappaltatore/sviluppatore: Dedalus Italia S.p.A. - P.IVA 05994810488
Giava - Vaccinazioni	INDRA ITALIA S.P.A.
SIRS - Sistema per gli screening oncologici	Enterprise Services Italia S.r.l.
SIMS - Sistema informativo per la medicina dello sport	RTI DEDAGROUP S.p.A. - ENTERPRISE SERVICES ITALIA S.R.L.
IRIS - Sistema Informativo IRIS “Infection Regional Information System”	Almaviva S.p.A.,
COReHealth	Dedalus S.p.A.

Assetto applicativo attuale della CCE

La CCE della Regione Puglia è stata realizzata per essere uno dei pilastri del sistema integrato di Sanità digitale regionale e per essere utilizzata come strumento per la gestione organica e strutturata dei dati riferiti alla storia clinica di un paziente in regime di ricovero o ambulatoriale. La CCE ha avuto come obiettivo by design quello di fornire un supporto trasversale ai percorsi di degenza e ambulatoriali, sia ospedalieri che territoriali e di disporre, a livello logico, di un unico strumento clinico per una gestione informatizzata, uniforme, aggiornata e integrata di tutto il ciclo di assistenza dei pazienti. Il Sistema Informativo (SI) di Cartella Clinica Elettronica, di ricovero e ambulatoriale è stato completato anche da un sistema centralizzato aziendale di richieste di prestazioni specialistiche e/o diagnostiche, chiamato Order Manager, al servizio di tutti i Sistemi Informativi che effettuano ‘richieste’ verso sistemi terzi, da un Repository clinico aziendale e da un sistema aziendale di Gestione dei Consensi, oltre che da una componente per la prescrizione dematerializzata.

Il Repository Clinico Aziendale contiene referti prodotti dai Sistemi Informativi sanitari aziendali e regionali e a tendere, grazie ai servizi richiesti con codesto AS contiene anche i dati strutturati di eventi clinici, unitamente con la definizione delle regole di pubblicazione e condivisione dei documenti e metadati ed è stato realizzato in modo tale che possa implementare il Dossier Sanitario Elettronico del singolo assistito, garantendo così che ci sia una circolarità delle informazioni cliniche tra le strutture sanitarie della medesima Azienda Sanitaria. Inoltre, il Repository è stato realizzato per essere un collettore dei documenti clinici prodotti da tutti i sistemi dipartimentali dell’Azienda Sanitaria e come l’unico alimentatore a livello aziendale del Fascicolo Sanitario Elettronico.

Per completare la gestione informatizzata dell’intero processo diagnostico-terapeutico-assistenziale ospedaliero è stato realizzato un sistema di gestione del Blocco Operatorio. Infine, sono state rese disponibili a corredo del

progetto tutte quelle componenti necessarie a gestire i livelli di sicurezza per gli utenti attraverso l'autenticazione e firma digitale con token o con autenticazione remota a due fattori, secondo quanto disposto dalle norme nazionali ed europee sul tema.

Sono state inoltre sviluppate le verticalizzazioni della Cartella Clinica Elettronica di ricovero e ambulatoriale relativamente alle seguenti discipline: cardiologia, ortopedia e traumatologia, terapia intensiva (al netto delle integrazioni con i monitor e i ventilatori), ostetricia e ginecologia, pediatria e neonatologia, diabetologia, disturbi cognitivi minori, oncologia e gestione UFA e nefrologia (quest'ultima solo relativamente alla scheda di anamnesi ed esame obiettivo).
Partendo dall'intervento già avviato e in virtù dell'articolato programma di ammodernamento e innovazione dei sistemi informatici sanitari regionali e delle aziende sanitarie pugliesi, l'Amministrazione intende evolvere e arricchire lo strumento di Cartella Clinica Elettronica regionale consolidandone il valore nel dominio dell'attività clinica e favorendo un'evoluzione che lo renda il perno di un sistema sempre più integrato con il dominio dell'assistenza territoriale. Inoltre, si intende realizzare un modello di monitoraggio e controllo che sia una leva per accelerare il processo di cambiamento, radicare capacità di autoanalisi e governo dei dati e introdurre metodologie di programmazione, verifica, confronto, valutazione e analisi del dato sanitario.

Per perseguire tali obiettivi si intende, in linea con quanto previsto dall' Accordo Quadro Consip denominato Sanità Digitale 1 (AQ SD1): implementare degli interventi di evoluzione relativi alle sopramenzionate piattaforme abilitanti dell'ecosistema sanità regionale, tesi a garantire il perseguimento di un modello gestionale integrato della continuità ospedale-territorio; implementare uno strumento di monitoraggio volto alla valorizzazione dei dati clinico-sanitari per abilitare e garantire modelli di assistenza innovativi e altamente integrati tra i diversi setting assistenziali; permettere un'analisi evoluta a supporto del governo della dimensione territoriale del SSR, nonché la definizione ed attuazione di efficienti modelli di interoperabilità del dato volti all'evoluzione dell'ecosistema regionale dei servizi digitali della Sanità, anche nel contesto di sviluppo delle piattaforme abilitanti nazionali e delle iniziative per lo sviluppo della telemedicina.

Dimensionamento della soluzione architetturale

Il Datacenter della Regione Puglia

Il datacenter della Regione Puglia, gestito da InnovaPuglia, è costituito da due CED in alta affidabilità e continuità operativa ed eroga risorse cloud secondo il paradigma IaaS (Infrastructure as a Service). Sarà reso disponibile un sito di Disaster Recovery, qualificato ai fini ACN, presso il quale l'aggiudicatario dovrà installare le relative componenti dell'applicazione per garantire, in caso di disastro, l'attivazione delle relative procedure per assicurare la continuità operativa del sistema CCE. Il Datacenter della Regione Puglia si occupa di monitorare le componenti infrastrutturali di erogazione dei servizi cloud. Qualunque tipo di monitoraggio delle applicazioni o sistemi informativi forniti sono a carico dell'aggiudicatario.
I CED sono ubicati presso la sede di Valenzano della in-house della Regione Puglia, InnovaPuglia S.p.A., in S.P. per Casamassima Km.3.
L'aggiudicatario dovrà installare tutte le componenti fornite su infrastrutture virtuali messe a disposizione da Regione Puglia presso il proprio Datacenter e nel sito di Disaster Recovery. Le risorse fornite saranno coerenti rispetto al disegno architetturale fornito in offerta e secondo il dimensionamento e la scalabilità indicata. Le procedure di richiesta ed attivazione delle risorse sono a carico dell'aggiudicatario e dovranno essere eseguite secondo il Regolamento Cloud del Datacenter della regione Puglia disponibile al link https://www.innova.puglia.it/web/guest/cloud-innovapuglia.
L' Infrastruttura IaaS del Cloud Il Datacenter della Regione Puglia è costituito da molteplici componenti hardware e software sui quali si basano i servizi cloud a paradigma IaaS forniti; di seguito sono riportate le tecnologie utilizzate a livello infrastrutturale e quelle più comuni a livello di middleware.

Ta

Tabella X: componenti hardware e software dei servizi cloud del datacenter regionale

La tabella deve servire unicamente come riferimento per l'offerente rispetto all'ambiente tecnologico in cui si andranno ad inserire i sistemi informativi offerti; pertanto, essa non è vincolante, al fine della redazione dell'offerta tecnica, rispetto alla selezione delle architetture tecnologiche scelte dall'offerente.

Dimensionamento dell'infrastruttura

Il Fornitore, a partire dalla soluzione applicativa proposta, dovrà indicare il dimensionamento delle componenti infrastrutturali necessarie all'erogazione degli ambienti di Produzione, Pre-produzione, Monitoraggio ed Addestramento del sistema Cartella Clinica Elettronica oltre che il dimensionamento dell'infrastruttura di Disaster Recovery (DR) per l'ambiente di Produzione. Gli ambienti di Produzione, Pre-produzione, Monitoraggio ed Addestramento saranno resi disponibili sull'infrastruttura del Datacenter della Regione Puglia.

Per componenti infrastrutturali s'intende:

- capacità di calcolo complessiva indicata in numero di Server Virtuali, con indicazione delle vCPU e dei vCore per ognuno di essi, verificando in fase esecutiva con il gestore del Datacenter (InnovaPuglia) i limiti fisici degli host hypervisor e quindi il numero massimo di vCPU assegnabili; e in ogni caso agendo principalmente sul paradigma della scalabilità orizzontale più che verticale in quanto più adatta ad ambienti Cloud;
- memoria RAM per ciascun Server Virtuale, verificando in fase esecutiva con il gestore del Datacenter (InnovaPuglia) i limiti fisici degli host hypervisor e quindi il numero massimo di vRAM assegnabile; e in ogni caso agendo principalmente sul paradigma della scalabilità orizzontale più che verticale in quanto più adatta ad ambienti Cloud;
- indicazioni del workload richiesto (vCPU e RAM) per ogni singolo modulo o componente/container che compongono la soluzione applicativa;
- spazio Disco necessario per ogni Server Virtuale oltre allo spazio disco necessario anche per aree condivise e per i Backup dei sistemi con indicazione della tipologia di storage (es. Object Storage, Block Storage, NAS) e delle performance minime richieste in termini di I/O e Throughput.
- banda di rete (inbound/outbound) minima richiesta per l'erogazione dei servizi.

Il dimensionamento della soluzione proposta dovrà rispettare i principi di scalabilità orizzontale dei servizi erogati. Pertanto, la proposta di dimensionamento dovrà essere fatta considerando le risorse necessarie per l'avvio del sistema con la possibilità di scalare all'aumentare del carico del lavoro. Rispetto al dispiegamento delle risorse infrastrutturali richieste, dovrà essere redatto un documento in cui si relazionerà nel merito dell'effettiva necessità delle risorse al momento della installazione e per un periodo di 6-12 mesi rispetto anche alle previsioni di utilizzo da parte degli utenti fornite dalla Stazione Appaltante. Pertanto, le risorse dovranno essere richieste in coerenza all'utilizzo atteso dei sistemi e dovranno essere dimensionate coerentemente con quanto dichiarato in offerta tecnica rispetto alle necessità computazionali e di storage delle applicazioni fornite e dovrà essere redatta una relazione tecnica che associ in maniera congrua le risorse richieste e l'obiettivo di carico/utilizzo della applicazione.

Le componenti software di base, del middleware ed applicative dovranno soddisfare tutti i requisiti di sicurezza stabiliti da ACN rispetto ai dati critici, ai sensi della Determina ACN n. 306.
Il Fornitore dovrà concordare con la Stazione Appaltante l'implementazione delle relative policies in termini di frequenza, retention e cifratura dei backup stessi.
L'approvvigionamento delle licenze (con relative manutenzioni per tutta la durata della fornitura) o le subscription per qualunque software inserito in offerta tecnica sarà a carico del Fornitore della Soluzione. Le uniche subscription che possono essere fornite dal Datacenter della Regione Puglia sono:

- Licenze di sistema operativo RedHat;
- Licenze di sistema operativo Microsoft Windows;
- Database Oracle Enterprise (senza ulteriori opzioni).

Il set-up, la configurazione e l'installazione delle varie componenti di tutta la soluzione, dovrà essere svolto dal Fornitore.
Il Fornitore dovrà proporre per la Soluzione anche la modalità con cui verrà eseguito l'allineamento dei dati con il sito di Disaster Recovery (DR) e le modalità di attivazione di tale sito in modo da garantire livelli di Recovery Point Objective (RPO) e Recovery Time Objective (RTO) in linea con la criticità del Servizio (RPO massimo 15 secondi e RTO massimo 30 minuti). Il Fornitore sarà tenuto allo svolgimento dei test di DR, previo accordo con la Stazione Appaltante, per valutarne l'effettivo funzionamento almeno a cadenza annuale. Sarà a cura del Fornitore la redazione del Piano di Disaster Recovery del Servizio oggetto della Fornitura.
Il dimensionamento proposto dal Fornitore verrà analizzato a cadenza trimestrale tramite i report che dovranno essere implementati dal Fornitore con gli strumenti di Capacity.
In caso di dimensionamento sovrastimato (≥30% di ogni risorsa infrastrutturale inutilizzata, ad esclusione della banda di rete, nel trimestre di analisi), il Fornitore sarà tenuto a giustificare la scelta del dimensionamento infrastrutturale proposto e dovrà provvedere alla formulazione di una proposta di ridimensionamento da sottoporre alla Stazione Appaltante. Tale ridimensionamento dovrà obbligatoriamente seguire il normale processo di Change Management.
Il Fornitore dovrà altresì produrre e manutenere la documentazione di progettazione infrastrutturale e applicativa (Request For Change) in continuità con gli standard ed i processi in uso presso la Stazione Appaltante, al fine di tenere traccia dell'evoluzione dell'infrastruttura del progetto e della sua realizzazione.

Tabella dei Requisiti infrastrutturali

ID	Ambito	Requisito
RI1	Infrastruttura	L'aggiudicatario dovrà produrre e tenere aggiornata tutta la documentazione richiesta dal Datacenter della Regione Puglia necessaria per il rilascio delle risorse cloud necessarie al servizio fornito
RI2	Infrastruttura	Il servizio deve prevedere le attività di set up e configurazione dell'infrastruttura. Nel dettaglio, il fornitore dovrà prevedere l'installazione di tutto il software necessario, inclusi i sistemi operativi.
RI3	Infrastruttura	Redazione del documento di dimensionamento delle componenti infrastrutturali che dovrà prevedere un piano di attivazione delle risorse in dipendenza dell'attivazione dei vari servizi rispetto all'attivazione del servizio per le diverse strutture pubbliche e private.
RI4	Infrastruttura	Redazione delle policies di backup
RI5	Infrastruttura	Redazione del Piano di Disaster Recovery
RI6	Infrastruttura	Redazione documento di progettazione infrastrutturale ed applicativa

RI7	Infrastruttura	Il servizio deve prevedere le attività di installazione, gestione e manutenzione dei servizi di monitoraggio dei servizi offerti e dovrà fornire alla Stazione Appaltante una dashboard di monitoraggio dello stato di funzionamento della applicazione
RI8	Infrastruttura	Il Fornitore deve fornire lo strumento di ticketing per la gestione dei processi di incident, change, configuration e problem management con piena visibilità alla Stazione Appaltante sullo stato e la lavorazione dei ticket per la quale dovrà essere fornito report trimestrale per la valutazione dei livelli di servizio.
RI9	Infrastruttura	Il Fornitore deve fornire documentazione dei processi che intende attuare per le attività di supporto alla continuità di servizio nonché RPO, RTO
RI10	Infrastruttura	Il Fornitore dovrà verificare semestralmente l'effettivo utilizzo delle risorse cloud richieste e, in caso di sotto-utilizzo per un periodo prolungato dovrà provvedere alla formulazione di una proposta di ridimensionamento da sottoporre alla Stazione Appaltante al fine di rilasciare le risorse non utilizzate.
RI10	Infrastruttura	Il Fornitore deve effettuare periodicamente dei test di restore a partire dai backup effettuati. Inoltre dovrà fornire reportistica relativa ai test effettuati e ai risultati ottenuti.
RI11	Infrastruttura	Il Fornitore dovrà rispettare, sul sistema complessivo e quindi su tutti i sistemi, il provvedimento del 27 novembre 2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga dei termini per il loro adempimento modificato dal provvedimento del 26 giugno 2009

Tabella 3: Tabella dei Requisiti Infrastrutturali (RI)

Ambiente di runtime

Per ambiente di runtime si intende l'infrastruttura tecnologica nella quale le componenti del sistema informatico operano e vengono eseguite. In questo contesto, l'ambiente di runtime può essere rappresentato da una macchina virtuale (virtual machine) o un contenitore (container). Entrambi forniscono un ambiente isolato e configurabile in cui le applicazioni possono essere eseguite.
Entrambe le opzioni hanno i propri vantaggi. La scelta dell'ambiente di runtime dipende dalle esigenze specifiche del sistema informatico, inclusi fattori come le prestazioni, l'isolamento, la gestione delle risorse e la flessibilità.
Per ciascuna componente del sistema, si richiede al Fornitore di indicare l'ambiente di runtime proposto, fornendo una motivazione oggettiva e ben argomentata per la scelta effettuata. È fondamentale che la motivazione consideri l'integrazione dell'ambiente di runtime con l'architettura e le specifiche del sistema proposto.

La motivazione deve comprendere diversi aspetti, tra cui:

- Prestazioni: l'impatto dell'ambiente di runtime sulla velocità di esecuzione delle componenti e sulla scalabilità del sistema.
- Isolamento: il grado di isolamento fornito dall'ambiente di runtime per garantire la sicurezza e la stabilità del sistema.
- Gestione delle risorse: la capacità dell'ambiente di runtime di gestire efficientemente le risorse del

sistema, come la memoria e il processore.
- Flessibilità: la facilità di configurazione e di gestione dell'ambiente di runtime, nonché la compatibilità con le tecnologie e gli strumenti utilizzati nel contesto del datacenter.
- Sicurezza: la sicurezza dell'ambiente di runtime proposto, compresa la protezione contro vulnerabilità, attacchi e intrusioni. Potrebbe essere importante considerare funzionalità come la gestione degli accessi, l'isolamento dei dati sensibili e le politiche di sicurezza implementate.
- Affidabilità: l'affidabilità dell'ambiente di runtime, compresa la tolleranza agli errori, la disponibilità e la capacità di ripristino in caso di guasti. È importante considerare la capacità dell'ambiente di runtime di gestire situazioni di emergenza e di mantenere la continuità del servizio.
- Scalabilità: la capacità dell'ambiente di runtime di scalare in modo efficiente per gestire carichi di lavoro crescenti. Ciò potrebbe includere la capacità di aggiungere risorse in modo dinamico, l'orchestrazione dei contenitori o l'elastico provisioning delle macchine virtuali per adattarsi alle esigenze di picco.
- Costi: i costi associati all'ambiente di runtime proposto, inclusi i costi di implementazione, manutenzione e gestione nel lungo termine. Il Fornitore deve essere in grado di dimostrare che la soluzione proposta offre un equilibrio tra prestazioni, funzionalità e costi.
- Esperienza e competenze del fornitore: l'esperienza e le competenze del Fornitore nell'implementazione e gestione dell'ambiente di runtime proposto.

Si richiede che la descrizione dei punti indicati sia strettamente legata e coerente con la soluzione applicativa proposta, al fine di fornire una valutazione approfondita e precisa delle scelte riguardanti l'ambiente di runtime. Le motivazioni fornite devono dimostrare una comprensione dettagliata delle esigenze specifiche del sistema e come l'ambiente di runtime proposto si integri in modo ottimale con la soluzione complessiva, garantendo prestazioni, sicurezza, scalabilità e una gestione efficiente delle risorse.
Si consiglia al fornitore di fornire esempi concreti, casi di studio o referenze che dimostrino la bontà della scelta proposta e l'adeguatezza dell'ambiente di runtime per soddisfare le esigenze specifiche del sistema.
La valutazione della soluzione proposta terrà conto della qualità e della completezza della motivazioni fornite dal fornitore e verranno presi in considerazione fattori di valutazione quali:

- Coerenza tra l'ambiente di runtime proposto e le specifiche tecniche del sistema;
- Solidità e completezza della motivazione fornita per la scelta dell'ambiente di runtime;
- Rilevanza delle considerazioni sulle prestazioni, sull'isolamento, sulla gestione delle risorse e sulla flessibilità;
- Compatibilità con le tecnologie e gli strumenti utilizzati nel contesto INNOVAPUGLIA;
- Costi associati all'implementazione, alla gestione e alla manutenzione dell'ambiente di runtime proposto.

Indipendentemente dall'ambiente di runtime scelto dal fornitore, il Datacenter della Regione Puglia fornirà sempre risorse cloud attraverso il paradigma IaaS, ovvero fornendo delle Macchine Virtuali. Il fornitore dovrà provvedere alla loro installazione e configurazione a partire dal sistema operativo.

Assetto infrastrutturale attuale della Cartella Clinica Elettronica

L'infrastruttura tecnologica è implementata con server virtuali e storage messi a disposizione nel Data Center Regionale presso la sede di InnovaPuglia. L'infrastruttura di produzione è distribuita sui due CED (A ed H) in continuità operativa.
Il Centro Servizi Cartella Clinica Elettronica è costituita dai seguenti ambienti:

- Ambiente di Esercizio
- Ambiente di Pre-esercizio
- Ambiente di Addestramento
- Ambiente di Monitoraggio

Lo schema architetturale dell'ambiente di esercizio è costituito da tre layers con distribuzione dei nodi nei due CED (A e H), segmentati per garantire i requisiti di sicurezza. Inoltre viene effettuato periodicamente un hardening dei sistemi al fine di eliminare potenziali vulnerabilità oltre ad implementare specifiche policies di accesso ed autenticazione. Tutte le componenti sono ridondate al fine di aumentare il grado di affidabilità e resilienza ad eventuali guasti e/o per attività di manutenzione; i nodi sono configurati in modalità active/active sui CED A e H con reindirizzamento automatico delle richieste in caso di fault di uno dei nodi attivi. Inoltre sono soddisfatti i requisiti di scalabilità sia orizzontale, con l'aggiunta, in caso di necessità di ulteriori nodi, che verticale, mediante il

potenziamento hardware di ciascun nodo.
Il sistema di pre-esercizio ha la stessa architettura logica dell'ambiente di produzione ma il dimensionamento dei sistemi, sia in termini di capacità elaborativa che di storage, è inferiore rispetto all'ambiente di produzione poiché i requisiti di carico sono evidentemente differenti.
Il sistema di addestramento ha la stessa architettura logica dell'ambiente di produzione, con un dimensionamento di capacità inferiore, e non è richiesto il meccanismo di alta disponibilità implementati sugli ambienti di produzione e di pre-esercizio.
E' presente un livello architetturale di Management sul quale sono attestati i sistemi di monitoraggio e di gestione.
Relativamente al servizio DataBase sono implementate le seguenti tecnologie:

- Postgre SQL;
- Oracle in modalità Real Application Cluster (RAC).

Il servizio di cartella clinica non è esposto su Internet per motivi di sicurezza, ma accessibile solo attraverso la rete RUPAR (Rete Unitaria della Pubblica Amministrazione Regionale) Puglia e la rete a larga banda regionale che collega le principali Strutture Sanitarie pugliesi ai servizi erogati dal Data Center Regionale. L'unica componente accessibile dalla rete Internet è il sistema di addestramento.

Dimensionamento delle macchine virtuali

Nelle tabelle seguenti è mostrato il dimensionamento fisico dei sistemi attualmente in esercizio.
Il dimensionamento della vRAM e del vDisk è espresso in Gigabyte, mentre, nella colonna Cloud SO, laddove non diversamente specificato, la lettera L significa che il sistema operativo è di tipo Linux.

Dimensionamento dell'ambiente di Produzione

Descrizione VM	inCloud Security Layer	inCloud SO	inCloud vCPU	inCloud vRAM	inCloud vDISK
WL1 Web Listener 1 WS-L001	WS-rupar	CentOS7	4	16	50
WL2 Web Listener 2 WS-L002	WS-rupar	CentOS7	4	16	50
WL3 Web Listener 1 new	WS-rupar	RedHat8	8	16 reserved	120
WL4 Web Listener 2 new	WS-rupar	RedHat8	8	16 reserved	120
REP1 AS Repository 1 AS-L001	AS	CentOS7	16	32 reserved	200
REP2 AS Repository 2 AS-L002	AS	CentOS7	16	32 reserved	200
CCE1 AS Cartella Clinica 1 AS-L003	AS	CentOS7	16	64 reserved	300
CCE2 AS Cartella Clinica 2 AS-L008	AS	CentOS7	16	64 reserved	300
CCE3 AS Cartella Clinica 3 AS-L013	AS	CentOS7	16	64 reserved	300
CCE4 AS Cartella Clinica 4 AS-L014	AS	CentOS7	16	64 reserved	300
CCEBAL1 Load Balancer 1 AS-L004	AS	CentOS7	8	16 reserved	100
CCEBAL2 Load Balancer 2 AS-L009	AS	CentOS7	8	16 reserved	100
PPR1 AS Prescrizioni 1 AS-L005	AS	CentOS7	16	48 reserved	200
PPR2 AS Prescrizioni 2 AS-L010	AS	CentOS7	16	48 reserved	200
SO1 AS Sale Operatorie 1 AS-L006	AS	CentOS7	8	64	100
SO2 AS Sale Operatorie 2 AS-L011	AS	CentOS7	8	64	100
UFA1 AS Accessi Chemioterapie 1 AS-L015	AS	CentOS7	8	16	100
UFA2 AS Accessi Chemioterapie 2 AS-L016	AS	CentOS7	8	16	100
MIR1 Mirth 1 AS-L007	AS	CentOS7	8	32	200
MIR2 Mirth 2 AS-L012	AS	CentOS7	8	32	200
DB1 Database Server 1 DB-L001	DB	OracleLinux8	32	192 reserved	220
DB2 Database Server 2 DB-L002	DB	OracleLinux8	32	192 reserved	220
DBQ Database Server Quorum DB-L003	DB	CentOS7	1	2	20
DBODT Diagnostic and Tuning pack DB-W001	DB	WinSrv19Std	4	16	180

Dimensionamento dell'ambiente di Monitoraggio

Descrizione VM	Cloud Business Group	Cloud Security Layer	Cloud SO	Cloud vCPU	Cloud vRAM	Cloud VM vDISK	Cloud WS Share NFS-HA	Cloud AS Share NFS-HA	Cloud DB Share NFS-HA	Cloud Backup Share NFS
RPU-CEM-WS-L001 WL1 Web listener	RPU-CEM	WS	L	4	8	50				
RPU-CEM-WS-L002 WL2 Web listener	RPU-CEM	WS	L	4	8	50				
RPU-CEM-AS-L001 SUP1 Supervisor	RPU-CEM	AS	L	4	16	50				
RPU-CEM-AS-L002 ELS1 Elastic search	RPU-CEM	AS	L	4	16	50				
RPU-CEM-AS-L003 GRF1 Grafana	RPU-CEM	AS	L	4	8	50				
RPU-CEM-AS-L004 SYSL1 Syslog	RPU-CEM	AS	L	4	16	120				
RPU-CEM-AS-L008 DNS1 FreeIPA	RPU-CEM	AS	L	4	8	100				
RPU-CEM-AS-L009 DNS2 FreeIPA	RPU-CEM	AS	L	4	8	100				
RPU-CEM-AS-L005 OTR1 OTRS	RPU-CEM	AS	L	4	8	200				
RPU-CEM-AS-L006 ZBX1 Zabbix	RPU-CEM	AS	L	4	8	100				
RPU-CEM-AS-L007 OSM1 Wazuh	RPU-CEM	AS	L	4	16	200				

Dimensionamento dell'ambiente di Addestramento

Descrizione VM	Cloud Business Group	Cloud Security Layer	Cloud SO	Cloud vCPU	Cloud vRAM	Cloud VM vDISK	Cloud WS Share NFS-HA	Cloud AS Share NFS-HA	Cloud DB Share NFS-HA	Cloud Backup Share NFS
WL1 Web Listener 1 WS-L001	RPU-CEA	WS	L	4	8	50				
WL2 Web Listener 2 WS-L002	RPU-CEA	WS	L	4	8	50				
REP1 AS Repository 1 AS-L001	RPU-CEA	AS	L	4	8	50				
SO1 AS Sale Operatorie 1 AS-L002	RPU-CEA	AS	L	4	8	50				
CCE1 AS Cartella Clinica 1 AS-L003	RPU-CEA	AS	L	8	16	100				
LEARN1 AS eLearning 1 AS-L004	RPU-CEA	AS	L	8	16	100				
CCEBAL1 Load Balancer 1 AS-L005	RPU-CEA	AS	L	4	8	30				
PPR1 AS Prescrizioni 1 AS-L006	RPU-CEA	AS	L	6	12	100				
MIR1 Mirth 1 AS-L007	RPU-CEA	AS	L	4	8	50				
DB1 Database Server 1 DB-L001	RPU-CEA	DB	L	4	8	500				500

Dimensionamento dell'ambiente di pre-esercizio

Descrizione VM	inCloud Security Layer	inCloud SO	inCloud Cluster	inCloud Load Balancer (solo per WS)	inCloud VIP	inCloud vCPU	inCloud vRAM	inCloud vDISK
WL1 Web Listener 1 WS-L003	WS-rupar	CentOS7	Cluster CED A		1	4	8	50
WL2 Web Listener 2 WS-L004	WS-rupar	CentOS7	Cluster CED H			4	8	50
WL3 Web Listener 1 new	WS-rupar	RedHat8	Cluster REDHAT - CED A		1	4	8	50
WL4 Web Listener 2 new	WS-rupar	RedHat8	Cluster REDHAT - CED H			4	8	50
REP1 AS Repository 1 AS-L002	AS	CentOS7	Cluster CED A		0	8	8	100
REP2 AS Repository 2 AS-L003	AS	CentOS7	Cluster CED H		0	8	8	100
CCE1 AS Cartella Clinica 1 AS-L004	AS	CentOS7	Cluster CED A		0	8	16	100
CCE2 AS Cartella Clinica 2 AS-L008	AS	CentOS7	Cluster CED H		0	8	16	100
CCEBAL1 Load Balancer 1 AS-L005	AS	CentOS7	Cluster CED A		0	4	8	50
CCEBAL2 Load Balancer 2 AS-L009	AS	CentOS7	Cluster CED H		0	4	8	50
PPR1 AS Prescrizioni 1 AS-L006	AS	CentOS7	Cluster CED A		0	8	32	60
PPR2 AS Prescrizioni 2 AS-L010	AS	CentOS7	Cluster CED H		0	8	32	60
SO1 AS Sale Operatorie 1 AS-L012	AS	CentOS7	Cluster CED A		0	4	8	60
SO2 AS Sale Operatorie 2 AS-L013	AS	CentOS7	Cluster CED H		0	4	8	60
MIR1 Mirth 1 AS-L007	AS	CentOS7	Cluster CED A		0	4	16	100
MIR2 Mirth 2 AS-L011	AS	CentOS7	Cluster CED H		0	4	16	100
DB1 Database Server 1 DB-L001	DB	OracleLinux8	Cluster ORACLEVM - CED A		5	8	24	200
DB2 Database Server 2 DB-L002	DB	OracleLinux8	Cluster ORACLEVM - CED H			8	24	200
DBQ Database Server - Quorum/Voting/NFS Oracle RAC	DB	CentOS7	Cluster 3S		0	1	2	20

Contesto organizzativo

Di seguito a titolo informativo si riporta il contesto organizzativo in cui insistono i servizi oggetto del presente AS. Si precisa che tale contesto potrebbe modificarsi nel corso della durata dell'esecuzione del contratto.

Contesto organizzativo di adesione al progetto di CCE di ricovero regionale	
Ente	**Presidio**
ASL BARI	Ospedale Di Venere Ospedale di Altamura Ospedale di Monopoli Ospedale San Paolo Corato

	Ospedale Fallacara Triggiano (Lungodegenza) Ospedale di Putignano Ospedale San Paolo Bari Ospedale San Paolo Molfetta Ospedale San Paolo Terlizzi Ospedale Monopoli-Fasano (di prossima apertura)
ASL BAT	Ospedale di Andria Ospedale di Andria (Plesso di Canosa) Ospedale Bisceglie Ospedale Barletta
ASL BRINDISI	Ospedale Perrino PO Francavilla Fontana Ospedale Ostuni
ASL LECCE	Ospedale di Gallipoli Ospedale Vito Fazi di Lecce Ospedale di Casarano Ospedale di Scorrano Ospedale di Galatina Ospedale di Copertino Ospedale di San Cesario
ASL TARANTO	Ospedale di Grottaglie Ospedale di Castellaneta Ospedale di Manduria Ospedale SS. ANNUNZIATA Ospedale Martina Franca Ospedale Taranto (Plesso Moscati)
IRCSS DE BELLIS	IRCSS DE BELLIS
IRCSS Istituto Tumori	IRCSS Istituto Tumori
AOU OSPEDALI RIUNITI di Foggia	AOU OSPEDALI RIUNITI di Foggia
ASL Foggia[1]	Ospedale di Cerignola Ospedale di San Severo Ospedale di Manfredonia
Totale presidi	**36**

Contesto organizzativo di adesione al progetto di CCA regionale		
Ente	**Tipologia presidio**	**Totale**
ASL BARI	*Ospedaliero* *Territoriale*	8 43
ASL BAT	*Ospedaliero* *Territoriale*	4 11
ASL BRINDISI	*Ospedaliero* *Territoriale*	3 20
ASL LECCE	*Ospedaliero*	7

[1] È previsto l'ingresso di ASL Foggia all'interno del progetto regionale di CCE a partire dal presente Appalto Specifico

	Territoriale	19
ASL TARANTO	*Ospedaliero*	6
	Territoriale	23
ASL FOGGIA[2]	*Ospedaliero*	3
	Territoriale	52
IRCSS DE BELLIS		1
IRCSS Giovanni Paolo II - Istituto Tumori		1
AOU OSPEDALI RIUNITI di Foggia		1
Totale presidi		**202**

Contesto organizzativo di adesione al progetto regionale in cui è previsto il Blocco Operatorio	
Ente	**Presidio**
ASL BARI	Ospedale Di Venere Bari Ospedale Fabio Perinei Altamura Ospedale di Monopoli Ospedale di Putignano Ospedale San Paolo
ASL BRINDISI	Ospedale Ostuni Ospedale Perrino Plesso San Pietro Vernotico Ospedale Perrino
ASL BAT	Ospedale di Barletta Ospedale Bonomo di Andria Ospedale di Bisceglie
ASL TARANTO	Ospedale di Manduria Ospedale Civile Martina Franca Ospedale. SS. ANNUNZIATA Ospedale di Castellaneta Ospedale di Grottaglie
IRCSS DE BELLIS	IRCCS De Bellis
IRCSS Giovanni Paolo II - Istituto Tumori	IRCCS Istituto Tumori
AOU OSPEDALI RIUNITI di Foggia	AOU OSPEDALI RIUNITI
ASL Foggia	Ospedale di San Severo Ospedale di Cerignola Ospedale di Manfredonia
Totale presidi	**19**

Ulteriori informazioni utili alla comprensione del contesto organizzativo riguardano le numeriche relative ai punti di erogazione e servizi definiti dalla programmazione regionale in applicazione del DM77/2022 di seguito riportate.

Case di Comunità	
ASL	**Numero CdC**
ASL BARI	36

[2] È previsto l'ingresso di ASL Foggia all'interno del progetto regionale di CCA a partire dal presente Appalto Specifico

ASL BAT	9
ASL TARANTO	18
ASL BRINDISI	9
ASL FOGGIA	27
ASL LECCE	24
Totale	**123**

Ospedali di Comunità	
ASL	**Numero OdC**
ASL BARI	13
ASL BAT	6
ASL TARANTO	6
ASL BRINDISI	7
ASL FOGGIA	9
ASL LECCE	6
Totale	**47**

Centrali Operative Territoriali	
ASL	**Numero COT**
ASL BARI	12
ASL BAT	5
ASL TARANTO	6
ASL BRINDISI	4
ASL FOGGIA	6
ASL LECCE	7
Totale	**40**
Consultori Familiari	
ASL	**Numero CF**
ASL BARI	37
ASL BAT	11
ASL TARANTO	16
ASL BRINDISI	16
ASL FOGGIA	28
ASL LECCE	35
Totale	**143**

Aspetti di innovazione e trasformazione digitale

L'intervento richiesto è finalizzato prioritariamente ad evolvere l'attuale sistema della Cartella Clinica Elettronica (CCE) regionale comprensivo di tutte le altre componenti (p.e. Order Manager, Repository, Clinico Aziendale, Blocco

Operatorio, ecc.) secondo un modello di progettazione esecutiva in grado di perseguire le prevedibili evoluzioni organizzative, di processo e tecnologiche. Gli interventi devono promuovere la valorizzazione del dato sanitario, in un'ottica funzionale all'analisi, programmazione e progettazione di azioni sistemiche a beneficio da un lato degli operatori sanitari facilitando le azioni quotidiane svolte dall'altro dei pazienti e della collettività. Gli interventi dovranno essere volti all'incremento della produttività del sistema sanitario complessivo, anche mediante la strutturazione di un sistema di supporto alle decisioni.
È altresì necessario ripensare la CCE aggiornando lo strumento esistente in una versione più evoluta, in linea con il fabbisogno generale socio-clinico-assistenziale favorendo l'integrazione con il sistema di assistenza territoriale e in coerenza con quanto definito nel DM77/2022 e nel Regolamento Regionale 13/2023 "Definizione di modelli e standard per lo sviluppo dell'assistenza territoriale ai sensi del DM 77/2022".

Gli interventi di sviluppo ed evoluzione della CCE avranno l'obiettivo di dotare gli operatori del SSR di uno strumento:

- Multidisciplinare, ovvero che si avvale dell'apporto di più discipline mediante l'acquisizione di dati sanitari in maniera trasversale;
- Multi-professionale, ovvero rivolta non solo ai medici ed infermieri, ma più in generale a tutti i professionisti e gli operatori sanitari, nel rispetto dei relativi ruoli e responsabilità;
- Multi-assistenziale, ovvero in grado di gestire differenti ambiti assistenziali, ospedalieri e territoriali (es emergenza e urgenza, ricoveri ospedalieri, le prestazioni di specialistica ambulatoriale);
- Longitudinale, ovvero che sia in grado di gestire e organizzare le informazioni e i dati clinici seguendo il percorso temporale del paziente, dalla nascita al fine vita;
- Multi-geografica, ovvero in grado di favorire la visibilità dei dati del paziente sia all'interno della stessa Azienda che tra Aziende.

Per quanto sopra, il progetto ha come obiettivo l'estensione funzionale della Cartella Clinica Elettronica, al fine di centralizzare tutte le attività cliniche in una soluzione unica regionale, resa disponibile in tutti i reparti e servizi delle strutture della Regione Puglia, e nello specifico

- Estendere e arricchire le applicazioni esistenti di nuove funzionalità della cartella clinica attualmente in uso quali ad esempio la gestione dei dati clinici del paziente che accede anche ai servizi di emergenza, la gestione della SDA, la funzionalità di Bed Management, la gestione del pre-ricovero e la gestione della Cartella della Salute Mentale e quella relativa alle Dipendenze Patologiche
- Gestire l'interoperabilità applicativa con i sistemi attualmente presenti in Regione Puglia o in via di sviluppo, per la condivisione delle informazioni cliniche raccolte nella Cartella Clinica unica, attraverso l'utilizzo di interfacce utente *standard* per una gestione integrata e completa delle informazioni del paziente.
- Estendere il dispiegamento delle funzionalità della cartella clinica affinché permetta di gestire in maniera continuativa il percorso e le informazioni relative al paziente durante la fase di deospedalizzazione, garantendo la convergenza dei bisogni dell'assistito con le necessità di condivisione e cooperazione tra team di figure sanitarie, sempre più allargati e dislocati sul territorio.
- Verticalizzare la Cartella Clinica Elettronica sulla base delle specifiche esigenze specialistiche che saranno a seguire esplicitate o che saranno raccolte in corso di progetto.

Da tali obiettivi scaturiranno molteplici *outcome* positivi e di notevole impatto per il paziente, l'utente e i gestori del dato clinico. Nello specifico la soluzione permetterà di:

- fornire agli utenti un ambiente di lavoro omogeneo, con la disponibilità di funzioni cliniche trasversali e condivise a livello aziendale e con un accesso controllato e contestuale a funzioni applicative specifiche per il contesto e ai dati clinici dei pazienti, che saranno storicizzati, aggregati e resi disponibili in maniera univoca per ciascun paziente
- esporre i dati e le funzionalità tramite interfacce *standard*, al fine di consentire una maggiore interoperabilità condividendo i dati raccolti e permettendo una gestione integrata e completa delle informazioni del paziente;
- eliminare progressivamente le chiamate di contesto nelle interazioni tra sistemi diversi (p.e. Cartella Clinica e Order Manager, Cartella Clinica e Gestore Consensi) a favore dell'implementazione di interfacce programmatiche *standard* (*web services*, HL7 *messaging*, ecc.) in accordo con quanto descritto nel punto precedente;

- garantire continuità con gli episodi ospedalieri del paziente tra i punti di erogazione all'interno della medesima Azienda ovvero in diverse Aziende, al fine di favorire la longitudinalità delle informazioni particolarmente importante nella gestione delle patologie croniche per la cura domiciliare ed il monitoraggio a distanza dell'assistito;
- consolidare e sviluppare le funzioni trasversali comuni ai diversi ambiti di applicazione (definizione piano terapeutico, erogazione della cura, diario medico ed infermieristico, ecc) e implementare funzioni preposte all'ambito specialistico nel quale verrà utilizzata.

Dal punto di vista architetturale e tecnologico, l'evoluzione della Cartella clinica dovrà permettere:

- l'interoperabilità applicativa con i sistemi attualmente presenti in Regione Puglia e in via di sviluppo, per lo scambio reciproco delle informazioni, grazie alla condivisione di dati strutturati e non, tramite cooperazione secondo lo *standard* sviluppato da HL7 "Repository FHIR". Tale Repository sarà componente centrale e fondamentale dell'architettura, permettendo di creare un punto unico e centralizzato per l'interscambio delle informazioni tra le varie componenti applicative;
- la condivisione di dati raccolti puntualmente e in coerenza con la normativa *privacy*, permettendo a chi autorizzato e interessato di essere aggiornato in merito alla presenza di nuove informazioni e al tempo stesso di generare flussi informativi disaccoppiati di comunicazione verso sistemi esterni;
- di avere un punto unico di accesso e recupero del dato in *near real-time*, semplificando l'interazione tra i sistemi e lo scambio di informazioni comuni, evitando la duplicazione del dato e possibili incoerenze.

Nella fattispecie, si dovranno integrare (ovvero creare ove opportuno) nuove interfacce sistemiche con l'obiettivo di mettere a fattor comune i dati raccolti al fine di permettere una gestione integrata e completa delle informazioni del paziente con i singoli sistemi di Nefrologia, Medicina Trasfusionale, Salute Mentale, Dipendenze patologiche, Rete regionale per la malattia di Parkinson, Emogasanalisi, ecc., e di inviare i dati clinici raccolti dalla CCE al sistema Edotto per garantire la corretta gestione dei flussi informativi relativi per esempio ad EMUR (Emergenza Urgenza), schede implantologiche, schede di morte, CEDAP (Certificato di Assistenza di Parto), Interruzione Volontaria di Gravidanza (IVG) e Aborto Spontaneo.

3 OGGETTO E DURATA DELL'APPALTO SPECIFICO

Oggetto della fornitura

I sistemi proposti oltre a soddisfare i requisiti previsti nel Capitolato Tecnico Speciale – Lotti Applicativi 1-2-3-4 della Gara indetta da Consip (ID 2202 - GARA A PROCEDURA APERTA PER LA CONCLUSIONE DI UN ACCORDO QUADRO, AI SENSI DEL D.LGS. 50/2016 E S.M.I., AVENTE AD OGGETTO L'AFFIDAMENTO DI SERVIZI APPLICATIVI E L'AFFIDAMENTO DI SERVIZI DI SUPPORTO IN AMBITO «SANITA' DIGITALE - SISTEMI INFORMATIVI CLINICO-ASSISTENZIALI» PER LE PUBBLICHE AMMINISTRAZIONI DEL SSN), con particolare riferimento alle aree tematiche del Lotto 2 (Cartella Clinica Elettronica ed Enterprise Imaging – Centro-Sud), dovranno essere rispondenti ai requisiti funzionali e non funzionali indicati nei paragrafi a seguire organizzati per aree applicative.

Il presente AS ha ad oggetto i sistemi applicativi di Cartella Clinica Elettronica
La presente procedura ha come scopo l'acquisizione dei seguenti servizi:

- Servizio di Manutenzione Evolutiva di Applicazioni Esistenti (MEV)
- Configurazione e Personalizzazione di Soluzioni di terze parti/open source/riuso (PP)
- Manutenzione Adeguativa e Manutenzione Correttiva (MAD-MAC)
- Servizi di gestione applicativi e basi dati (GAB)
- Supporto Specialistico (SS)
- Servizi di Conduzione Tecnica (CT);
- Supporto Tecnologico (ST)
- Servizi accessori:
  - Servizi di Service Control Room per Monitoraggio tecnico/applicativo.

Durata del contratto

La durata del contratto esecutivo spiega i suoi effetti dalla data di conclusione delle attività di subentro ovvero, ove non ci sia stato subentro, dalla data di conclusione delle attività di set-up ed avrà termine allo spirare di 48 mesi salvi i casi di risoluzione o recesso ai sensi dell'Accordo Quadro e del Contratto Esecutivo.
L'Amministrazione, in conformità a quanto disposto all'articolo 106, comma 11, del D. Lgs. n. 50/2016, si riserva la facoltà in corso di esecuzione di modificare la durata del Contratto Esecutivo, con comunicazione inviata a mezzo PEC al Fornitore, prorogandolo per il tempo strettamente necessario alla conclusione delle procedure necessarie per l'individuazione di un nuovo contraente, ivi inclusa la stipula del contratto. In tal caso il Fornitore è tenuto all'esecuzione delle prestazioni previste nel contratto agli stessi prezzi, patti e condizioni o più favorevoli per l'Amministrazione.

4 LUOGO DI ESECUZIONE DEI SERVIZI DI AS E STRUMENTI A SUPPORTO DELLA FORNITURA E OBBLIGHI GENERALI

Luogo della fornitura

I servizi oggetto del presente AS dovranno essere erogati in base alla tipologia di servizio:

- presso i punti di erogazione degli Enti del SSR, le sedi dell'Amministrazione e presso i locali che ospitano il Data Center di InnovaPuglia;
- presso le sedi del Fornitore.

Le attività da svolgersi presso le sedi dell'Amministrazione e/o della Committente dichiarate in AS non ammettono spese di trasferta, anche nel caso in cui ci sia l'esigenza di svolgere attività al di fuori della provincia di riferimento della sede indicata.

Strumenti a Supporto della Fornitura

Al fine di garantire una corretta governance delle attività previste nell'ambito della Fornitura, il Fornitore dovrà mettere a disposizione dell'Amministrazione, senza oneri aggiuntivi e per l'intera durata del contratto, uno strumento di Governo della Fornitura (SGF) attraverso il quale l'Amministrazione potrà avere una costante fotografia sempre aggiornata dello stato complessivo del progetto. Lo strumento di Governo della Fornitura dovrà essere dettagliatamente descritto nell'Offerta Tecnica del Fornitore, dettagliando le funzioni che mette a disposizione.

5 DESCRIZIONE DEGLI OGGETTI DI FORNITURA

Requisiti funzionali

Servizi

Servizio di Manutenzione Evolutiva di Applicazioni Esistenti (MEV)

Il progetto evolutivo prevede l'evoluzione della Cartella Clinica Elettronica, attualmente realizzata, comprensiva di tutte le altre componenti SW (quali ad esempio l'Order Manager, il Blocco Operatorio, il Repository Clinico Aziendale, ecc.) per soddisfare le esigenze anche di altri setting assistenziali diversi da quelli di ricovero e ambulatoriale e per soddisfare ancor di più le esigenze degli utenti.

L'obiettivo è di avere un'unica soluzione integrata, focalizzata sulla centralità del dato così da limitare la duplicazione delle informazioni ed integrarle, aggregando le funzionalità necessarie per una completa gestione dei dati acquisiti durante l'intero percorso clinico.
La Cartella Clinica Elettronica conserverà i moduli trasversali già implementati estendendoli ai nuovi setting assistenziali e svilupperà funzionalità contestualizzate rispetto all'ambito in cui sarà dispiegata.
Per quanto attiene ai requisiti e modalità di erogazione del servizio, al team di lavoro e alle metriche di dimensionamento si rimanda a quanto presente nel CTS Lotti applicativi al capitolo 4 relativamente al servizio oggetto del presente paragrafo.

ESTENSIONE DELLA CARTELLA CLINICA ELETTRONICA VERSO IL SERVIZIO DI PRONTO SOCCORSO

Nel tempo il Pronto Soccorso ha subito un'evoluzione in larga parte determinata dalle pressioni sociali della moderna società. Il Pronto Soccorso si sta adeguando anche alla tipologia degli accessi che non sono soltanto interventi legati alle grandi emergenze (incidenti stradali, edema polmonare, infarto, ictus, ecc.) ma anche appunto al trattamento dei sintomi legati alle malattie croniche come ad es. le crisi respiratorie legate alla bronchite cronica fino al trattamento di episodi legati alle neoplasie.
In aggiunta a tale quadro occorre considerare un'altra tendenza del nostro SSN, che è quella della riduzione dei giorni di degenza e della deospedalizzazione, cui consegue la pratica, soprattutto nelle grandi strutture, di effettuare, in seguito ad un accesso in Pronto Soccorso, una degenza breve direttamente nel Pronto Soccorso in apposite sale in cui il paziente viene curato in modalità OBI (Osservazione Breve Intensiva) e sul quale viene definito dal medico di Pronto Soccorso un piano di cura poi attuato dagli infermieri rendendo il Pronto Soccorso come un "reparto" sempre più autosufficiente dell'Ospedale che deve dare risposte il più possibile complete rapide ed efficaci.
Il Pronto Soccorso è dunque, oggi, chiamato a riorganizzarsi anche rispetto a queste nuove necessità, strutturandosi come un reparto di cura eterogeneo e che deve utilizzare i più moderni concetti di Cartella Clinica Elettronica.
Il progetto evolutivo prevede, di conseguenza, l'estensione della Cartella Clinica Elettronica, attualmente utilizzata dalla Regione Puglia per i pazienti ricoverati e ambulatoriali, anche per la gestione dei pazienti che accedono ai servizi di emergenza/urgenza.
L'obiettivo è di avere all'interno della Cartella Clinica Elettronica un modulo di Pronto Soccorso che:

- gestisca tutti i processi e le funzionalità dell'attuale sistema presente per la gestione del Pronto Soccorso (Edotto), garantendo continuità funzionale rispetto al modulo già in uso;
- fornisca ulteriori funzionalità a supporto dei processi clinici (come più dettagliatamente descritto in seguito);
- includa gli strumenti necessari per l'alimentazione di piattaforme di DWH e BI oltre che ad eventuali strumenti di Data Analytics;
- estenda, su più servizi (reparto, ambulatorio, pronto soccorso, ecc) la stessa soluzione affinché più operatori possano beneficiare della stessa User eXperience nei diversi scenari d'uso.

Riusando le funzionalità già presenti nella Cartella Clinica Elettronica Regionale attualmente in uso e estendendola ove necessario, il modulo di pronto soccorso deve essere in grado di supportare il personale del pronto soccorso in tutte le attività orientate al paziente (raccolta dati anagrafici, triage, anamnesi, esame obiettivo, diario, richieste esami, raccolta consensi mediante integrazione col Gestore Consensi Aziendale, etc.), consentendo al tempo stesso l'invio dei dati raccolti dal nuovo modulo di Pronto Soccorso al sistema Edotto, per garantire la gestione dei flussi informativi regionali.
Di seguito alcune delle funzionalità che devono essere garantite:

- Mappa iconografica interattiva del Pronto Soccorso: la gestione organizzativa del Pronto Soccorso si baserà principalmente su una visione di insieme dei pazienti presi in carico dalla struttura rappresentata attraverso una mappa iconografica del Pronto Soccorso, suddiviso nei vari ambulatori di trattamento, i pazienti presenti e per ogni paziente gli eventuali allarmi ad evidenza di informazioni di rilevanza clinica (presenza di referti, di farmaci da somministrare, ecc.). Scopo funzionale della mappa è di fornire ai clinici una finestra di dialogo che consenta al medico o all'infermiere di visualizzare i pazienti divisi per sala accelerando in tal modo il processo di definizione delle priorità di presa in carico dei pazienti.
- Cartella medica: già sviluppata nell'attuale applicativo di Cartella Clinica Elettronica, la cartella medica, specializzata per il Pronto Soccorso ove necessario, permetterà di gestire le attività diagnostico/terapeutiche ed assistenziali svolte dal personale medico all'interno del Pronto Soccorso. Il

sistema supporterà gli operatori durante le attività di visita per la compilazione dell'anamnesi e dell'esame obiettivo, delle allergie e fattori di rischio, diario medico, prescrizione di attività e terapie, monitoring della cura (grafica terapia, cronologia dell'episodio).

- Cartella Infermieristica: già sviluppata nell'attuale applicativo di Cartella Clinica Elettronica, la cartella infermieristica, specializzata per il Pronto Soccorso ove necessario, sarà di supporto al personale infermieristico durante tutto l'episodio e prevederà che il personale infermieristico possa prendere in carico il paziente, registrando le informazioni di propria competenza sulla scheda infermieristica: scale di valutazione, somministrazione terapia farmacologica e registrazione dei parametri vitali rilevati, prestazioni effettuate in Pronto Soccorso, diario infermieristico, ed altri inserimenti di dati in forma strutturata.
- Lista di lavoro medica/infermieristica: funzionalità già sviluppata nell'attuale applicativo di Cartella Clinica Elettronica, sarà ove necessario specializzata per il Pronto Soccorso affinchè il sistema consenta nel modo più ottimale, di visualizzare la worklist delle attività medico/infermieristiche generate automaticamente dal sistema e permetterne la registrazione della relativa esecuzione.
- Allarmi e notifiche: funzionalità già sviluppata nell'attuale applicativo di Cartella Clinica Elettronica, sarà ove necessario specializzata per il Pronto Soccorso affinchè il sistema consenta di visualizzare nella maniera più ottimale per gli utenti del Pronto Soccorso, lo stato dei pazienti con l'evidenza di eventi quali la mancata somministrazione di terapie, arrivo di referti, parametri vitali fuori range, ecc.
- Foglio Unico Terapia (FUT): funzionalità già sviluppata nell'attuale applicativo di Cartella Clinica Elettronica, sarà ove necessario specializzata per il Pronto Soccorso per consentire nel modalità più consona, di visualizzare l'andamento temporale della terapia farmacologica durante tutto il corso della sua esecuzione, in relazione all'andamento temporale dei valori antropometrici, mediante una vista bidimensionale sul paziente.
- Diario di episodio: funzionalità già sviluppata nell'attuale applicativo di Cartella Clinica Elettronica, sarà ove necessario specializzata per il Pronto Soccorso per consentire di visualizzare la sequenza cronologica di notifiche di eventi di varia natura, con evidenza di relativo orario e autore. Il diario di episodio sarà alimentato in maniera automatica con tutti gli eventi clinici rilevati dal sistema durante l'episodio dall'atto dell'accettazione in poi (richieste di esami, e tutte le attività realizzate dal personale infermieristico come le rilevazioni dei parametri vitali, la somministrazione dei farmaci, ecc.), più tutte le annotazioni inserite manualmente dai clinici durante l'episodio.
- Gestione richieste: a supporto della gestione delle richieste di esami e visite, sarà utilizzato il sistema centralizzato di gestione di order entry e management, attualmente utilizzato già per la gestione dei ricoveri, per gestire il flusso di richieste di prestazioni dal pronto soccorso verso i servizi erogatori (radiologia, laboratorio, consulenze, ecc.) e le relative informazioni di ritorno (stato delle richieste, referti, immagini, allegati).

Il modulo di Pronto Soccorso, all'interno della Cartella Clinica Elettronica, deve inoltre dotato delle funzionalità di seguito descritte:

- Accettazione/Triage paziente: la funzione di accettazione consentirà di gestire il processo di accoglienza dei pazienti in Pronto soccorso. Verrà utilizzata dal personale preposto per registrare l'accesso del paziente e procedere al successivo indirizzamento dei pazienti verso gli ambulatori di competenza. L'operatore in questa fase avrà a disposizione strumenti che gli consentiranno di gestire i dati relativi all'accesso, quindi:
  - informazioni relative alla tipologia di assistenza del paziente;
  - la modalità di accesso al Pronto soccorso;
  - la dinamica e il luogo dell'evento;
  - una interfaccia guidata per l'assegnazione del codice di priorità di assistenza;
  - le informazioni relative ad un eventuale arrivo del paziente tramite il 118;
  - dati dell'accompagnatore;
  - dati clinici;
  - consensi.
- Osservazione Breve Intensiva: il modulo deve consentire la gestione del percorso clinico diagnostico dei pazienti che hanno effettuato un accesso in pronto soccorso e per i quali è necessario, ai fini di un approfondimento diagnostico, un breve periodo di osservazione. La gestione clinica del paziente dovrà

essere realizzata con le stesse funzioni utilizzate per il paziente non in OBI, compresa la gestione delle richieste di Esami e Consulenze, così da avere una continuità sia operativa da parte degli operatori che una continuità di raccolta di dati clinici del paziente.

- Dimissione del paziente: il sistema supporterà i medici nelle attività di dimissione del paziente attraverso l'inserimento delle informazioni necessarie alla chiusura e relativa apposizione della firma digitale al verbale di pronto soccorso che deve essere inviato al Repository Clinico Aziendale (per il successivo invio a FSE o indicizzazione in FSE) già a disposizione delle Aziende Sanitarie che utilizzano la CCE regionale. Tutte le informazioni precedentemente inserite, o registrate anche tramite integrazioni con altri sistemi, saranno messe a disposizione automaticamente dal sistema per la compilazione del verbale di pronto soccorso, evitando le trascrizioni manuali dei dati. Sarà gestita la documentazione amministrativa correlata all'episodio (INAIL, incidente stradale/domestico, denuncia di morso o graffio animale, invio certificato di malattia) e l'emissione dell'invito al pagamento (ticket). Qualora l'episodio di pronto soccorso si concluda con la necessità di un ricovero, l'applicativo dovrà colloquiare opportunamente con la componente di ADT di CCE e garantire l'accettazione del ricovero e la trasmissione automatica dei dati al reparto di destinazione tramite l'applicativo di CCE, nonché consentire al reparto di destinazione l'accesso a tutti i documenti e i dati prodotti durante l'episodio di pronto soccorso.
- Gestione dei Consensi: l'implementazione delle funzionalità di Pronto Soccorso come componente interna alla Cartella Clinica Elettronica deve prevedere le necessarie integrazioni con il Sistema di Gestione dei Consensi di livello Aziendale. I servizi del Gestore Consensi, utili per l'acquisizione e la verifica dei consensi liberi e informati (p.e. consenso informato alla prestazione sanitaria) devono essere fruiti dalla componente di Pronto Soccorso in tutti i casi d'uso in cui è possibile raccogliere la volontà del paziente.
- Integrazione con il Sistema Informatico di CO 118: l'integrazione delle funzionalità del Servizio di Pronto Soccorso con la Centrale Operativa del 118 deve prevedere, almeno, la ricezione in CCE della Scheda Paziente Digitale (SPD 118). La SPD 118 colleziona tutte le informazioni relative all'evento di soccorso quali: identificativo evento, anagrafica paziente, valutazione sanitaria sul posto di soccorso (parametri vitali, diagnosi, dati clinici, ecc.), terapia attuata, farmaci somministrati e codice di gravità assegnato. Alla SPD 118 possono essere associati anche alcuni allegati quale, per esempio, il referto ECG prodotto dal Sistema di Telecardiologia. L'integrazione e la condivisione della SPD 118 consentirà, già nelle prime fasi del trasporto e dal mezzo di soccorso, di preallertare il Pronto Soccorso consentendo di organizzare al meglio l'accettazione del paziente ancor prima dell'arrivo dello stesso in PS.

Il fornitore dovrà presentare la stima dell'intervento entro il termine massimo di 2 mesi dalla data di stipula del contratto; il collaudo funzionale dovrà essere effettuato entro il termine massimo di 6 mesi dalla data di accettazione del documento di stima.

GESTIONE AMMINISTRATIVA DEL PRE-RICOVERO

Il Sistema deve consentire la gestione delle prenotazioni per il pre-ricovero finalizzato ad esempio agli interventi chirurgici. A titolo esemplificativo e non esaustivo dovranno essere gestiti: l'agenda delle disponibilità delle prestazioni, la pianificazione dei pre-ricoveri, la registrazione della comunicazione delle date all'assistito, la modalità di comunicazione, meccanismi di notifica in prossimità della data pianificata (p.es. tramite mail o sms), ecc.

MONITORAGGIO OCCUPAZIONE DEI POSTI LETTO

Il progetto evolutivo prevede l'estensione della Cartella Clinica Elettronica con funzionalità dedicate al Bed Management. Il modulo deve

- permettere la gestione dei processi che regolano l'allocazione, la permanenza e il trasferimento interno del paziente nel singolo Presidio Ospedaliero ma anche in quelli appartenenti alla stessa Azienda anche per il tramite di un cruscotto che consenta di visualizzare l'occupazione dei posti letto complessiva;
- regolare un insieme di procedure e standard coerenti con le dotazioni e le attività cliniche delle unità organizzative assegnando ad ogni paziente il posto più congruo per intensità di cura e per competenza specialistica;
- consentire di aggiungere il dato di previsione della dimissione ai fini di favorire i processi di *transitional*

care;

- permettere di assicurare nei tempi stabiliti, il ricovero da PS nei reparti di degenza o il trasferimento tra reparti, verificando in tempo reale lo stato di occupazione dei posti letto e monitorando le dimissioni giornaliere, comunicando, qualora fosse possibile con la Centrale Operativa 118 della Provincia al fine di reindirizzare l'emergenza sulla struttura rispondente;
- consentire il monitoraggio dei principali indicatori relativi alla gestione dei posti letto, quali ad esempio il tasso di occupazione, la durata media della degenza, i ricoveri inappropriati.

GESTIONE DELLA SDA E COMUNICAZIONE DATI AD EDOTTO

In ottemperanza alla DGR n. 2774/2014, le strutture pubbliche e private accreditate sono tenute a completare l'inserimento dei dati relativi alle prestazioni specialistiche della tipologia "day-service" mediante la compilazione della SDA (scheda di day-service).
Per le strutture che erogano prestazioni di day-service, la CCE dovrà offrire la funzionalità di raccolta dei dati per la compilazione della scheda definita nella suddetta delibera e l'invio dei dati al sistema Edotto.

GESTIONE DELLA SDO-R

Il progetto evolutivo prevede l'estensione della Cartella Clinica Elettronica con funzionalità dedicate alla gestione dei pazienti che necessitano di un percorso clinico riabilitativo nei regimi di degenza ordinaria e day hospital. La cartella deve consentire di gestire le attività correlate ad un programma di riabilitazione "post-acuzie", ovvero realizzato nelle settimane immediatamente successive all'evento traumatico, sia un'attività assistenziale complessa, quindi rivolta a persone, adulti e bambini, con invalidità civile riconosciuta, ovvero la riabilitazione "estensiva" (servizio assistenziale "ex articolo 26").
La soluzione deve consentire la gestione della documentazione clinica correlata alla presa in carico dell'assistito da parte della struttura, e alla prima valutazione multidimensionale iniziale e predisposizione di un progetto riabilitativo individuale (PRI) nel caso di trattamenti riabilitativi intensivi o estensivi.
Ogni operatore, medico, infermiere, terapista, dovrà disporre della documentazione clinica di sua pertinenza, per esempio l'anamnesi, l'esame obiettivo, la valutazione di ingresso, la valutazione intermedia, la valutazione finale, il documento di apertura del progetto riabilitativo, ecc... Per la gestione del paziente riabilitativo la soluzione dovrà mettere a disposizione funzionalità che consentono di gestire la pianificazione delle attività di vita quotidiana (ADL) e gli interventi medici riabilitativi.
L'applicativo dovrà consentire la compilazione (ove possibile in maniera automatica a partire dai dati già inseriti) della SDO-R e poter inviare al sistema Edotto le informazioni per la generazione del flusso SIAR relativo al Sistema informativo per il monitoraggio dell'assistenza riabilitativa (SIAR) nell'ambito degli interventi previsti dal PNRR finalizzati a implementare modelli per l'analisi dei dati, la sorveglianza e vigilanza sanitaria e a garantire i Livelli Essenziali di Assistenza.

SVILUPPO VERTICALIZZAZIONI SPECIALISTICHE DI CCE

A completamento delle verticalizzazioni specialistiche già completate è richiesto lo sviluppo delle seguenti verticalizzazioni a titolo esemplificativo e non esaustivo:

- Terapia intensiva neonatale
- Oculistica (incluso la possibilità di eseguire disegni anatomici)
- Cardiochirurgia
- Reumatologia
- Fisiopatologia digestiva
- Cartella anestesiologica
- Chirurgia Generale
- Medicina Generale
- Urologia
- Neurologia
- Pneumologia
- Neurochirurgia

- Psichiatria
- Otorinolaringoiatria
- Gastroenterologia
- Malattie infettive
- Chirurgia vascolare
- Chirurgia plastica
- Chirurgia toracica
- Malattie endocrine e del sistema nutrizionale
- Geriatria
- Neuropsichiatria infantile
- Dermatologia
- Chirurgia pediatrica
- Oncoematologia pediatrica
- Grandi ustionati
- Odontoiatria e stomatologia
- Unità spinale
- Neuroriabilitazione

Si potranno richiedere migliorire anche sulle verticalizzazioni esistenti.

GESTIONE DELLA PRESA IN CARICO

Ai fini di una migliore gestione della presa in carico dei pazienti e di gestione del percorso diagnostico-terapeutico la CCE deve poter rilevare l'informazione dello status delle prestazioni prenotate tramite la stessa CCE.

ASSISTENTE VIRTUALE

Si richiede lo sviluppo all'interno della CCE della funzionalità di assistente virtuale per l'utente a supporto dell'utilizzo e della conoscenza delle funzionalità e delle caratteristiche di CCE. La soluzione deve avere almeno i seguenti requisiti:

- presentare un'interfaccia utente facile da navigare sia per l'*input* testuale che vocale;
- essere facilmente accessibile dall'applicativo della CCE senza richiedere l'apertura di software o applicazioni esterne;
- funzionare su diversi dispositivi utilizzati dagli operatori sanitari, inclusi *desktop*, *laptop*, *tablet* e smartphone;
- essere capace di riconoscere e processare *input* sia in forma scritta che vocale;
- riconoscere e rispondere in più lingue per accomodare una vasta gamma di operatori sanitari;
- essere capace di comprendere, analizzare e rispondere a domande relative al funzionamento di CCE, all'uso improprio della stessa e suggerire modalità di utilizzo corrette;
- fornire risposte diversificate in base alla tipologia di utente del servizio;
- utilizzare tecniche *Natural Language Process* (NLP) avanzate per comprendere con precisione le domande degli utenti in linguaggio naturale;
- garantire la disponibilità del servizio 24/7, con tempi di inattività minimi;
- essere capace di gestire un alto numero di interrogazioni simultaneamente senza degradare le *performance*;
- ridurre al minimo il tempo di attesa per le risposte per non interrompere i flussi di lavoro degli operatori sanitari.

CRUSCOTTO DI MONITORAGGIO

Per consentire l'analisi di peculiari fenomeni clinico-sanitari, monitorare i principali indicatori di performance e fornire agli utenti innovativi strumenti di fruizione del contenuto informativo garantendo il corretto accesso ai dati di propria competenza, si prevede la realizzazione di un cruscotto che consenta in maniera dinamica, pratica e personalizzabile:

- il monitoraggio dell'utilizzo delle componenti applicative (p.es. CCE di ricovero e ambulatoriale, Gestore consensi aziendale, prescrizione dematerializzata, blocco operatorio, ecc.), considerando ad esempio il

numero di utenti univoci che hanno avuto accesso al sistema rispetto a quelli censiti per presidio e reparto, il tasso di accesso al sistema, ovvero la frequenza con cui gli utenti accedono al sistema per presidio e reparto, il tempo medio di utilizzo del sistema per presidio e reparto, la percentuale di funzionalità utilizzate rispetto a quelle disponibili per presidio e reparto, il numero di documenti prodotti distinti per tipologia e stato, il numero medio di allegati per cartella, il numero di richieste effettuate tramite order entry da parte di ciascun reparto/PS, il numero di interventi di sala registrati sul totale degli interventi effettuati, il numero di consulenze richieste tramite CCE sul totale, il tempo di attività e inattività del sistema, il numero dei documenti prodotti e conferiti a FSE

- il monitoraggio delle performance del sistema in termini di tempo risposta delle funzionalità utilizzate, attraverso in cruscotto ad utilizzo di utenti specifici delle Aziende Sanitarie e della Regione;
- la consultazione di dati utili al controllo di gestione delle Aziende Sanitarie, a titolo esemplificativo e non esaustivo, dati di occupazione in tempo reale dei posti letto, dati sulle prestazioni erogate (es. degenza media, tipo di DRG e regime), numero di accessi ripetuti, numero di prestazioni per interni richieste ed eseguite, calcolo del costo medio di farmaci per giornata di degenza, gestione di dati utili alla verifica dell'appropriatezza dei ricoveri e/o delle procedure ecc.
- la realizzazione di data-mart verticali, a supporto delle analisi degli utenti, specializzati sulle aree tematiche citate tra gli obiettivi e di data-mart multi-sorgente per analisi avanzate sul Fabbisogno Sanitario e del consumo delle prestazioni sanitarie del SSR e realizzazione di specifiche aree con indicatori e KPI progettati per l'analisi di particolari fenomeni di interesse
- il supporto all'ente nella preparazione dei dati nella DataPlatform Regionale, per abilitare la generazione autonoma di reportistica e dashboards sui diversi domini informativi e la loro successiva distribuzione
- la realizzazione di procedure/API automatizzate, per il controllo della qualità dei dati e per l'invio di dati e metadati per consentire eventualmente il colloquio dei principali protocolli clinici come FHIR e HL7 verso la DataPlatform Regionale con l'obiettivo di ottenere una centralizzazione delle anagrafiche.
- la realizzazione di dashboard e report con dati a forte connotazione geografica (a titolo di esempio non esaustivo si citano: distribuzioni geografica della provenienza dei pazienti per diagnosi, concentrazioni di morbilità, ecc.).

EVOLUZIONE DEL REPOSITORY AZIENDALE *FHIrR*

Nell'ambito della gestione e archiviazione di documenti e dati, ad oggi, si riscontra una complessa situazione di disomogeneità che riguarda sia aspetti relativi ai producer (legati alla mancanza della gestione del dato strutturato neidocumenti clinici e alla non completa gestione del nucleo minimo documentale), cheai consumer (dipendenti dalla diversa diffusione e fruizione dei servizi per l'accesso e la consultazione dei dati).

Il presente paragrafo propone gli interventi necessari e le azioni mirate per l'evoluzione, del contesto attuale, in una direzione di maggior condivisione e razionalizzazione dei dati finalizzati al conferimento verso FSE 2.0.

Si precisa che l'approccio architetturale deve essere in accordo con lo "Studio di Fattibilità FSE 2.0" già sviluppato dal precedente Fornitore CCE e approvato da Regione Puglia nel corso del precedente contratto.

La strategia proposta, per rendere l'attuale modello architetturale regionale compliant al modello FSE 2.0, vedrà un rafforzamento del Repository Documentale Aziendale (RDA), dal punto di vista dei contenuti informativi archiviati e gestiti, e l'introduzione del Clinical Data Repository Aziendale (CDRA) per la gestione dei dati secondo lo standard FHIR.

Allo scopo di alimentare il Fascicolo Sanitario Elettronico in modalità diretta e real-time, si precisa che la logica di alimentazione di quest'ultimo dovrà essere implementata direttamente dal Repository Documentale Aziendale.

Il rafforzamento del Repository Aziendale (RDA) e l'introduzione dei Clinical Data Repository sarà concentrato sul potenziamento di quei fattori che consentono di avere a disposizione dati completi, affidabili ed efficaci, requisito fondamentale per la messa in atto del modello di interoperabilità proposto con l'architettura FSE 2.0.

La soluzione proposta, per l'architettura del repository dei documenti e del CDR, indirizza quindi i seguenti obiettivi:

- gestione documentale e dei dati clinici organizzata, omogenea e organica, mediante integrazione con i producer per l'acquisizione dei contenuti già previsti dalle linee guida del FSE 2.0 e di eventuali ulteriori contenuti informativi con possibili integrazioni future;
- predisposizione di una architettura coerente con quanto previsto dalle linee guida di attuazione del Fascicolo Sanitario Elettronico 2.0 (FSE).

Si prevede, inoltre, l'implementazione di un Repository aziendale FHIR per l'archiviazione e la condivisione dei dati clinici, prodotti nei contatti tra i pazienti e le strutture ospedaliere e sanitarie durante il percorso diagnostico terapeutico, che consentirà la visibilità completa e un supporto all'interoperabilità tra i sistemi.
Con la finalità di dotare la Regione Puglia di uno strumento aziendale unico e centralizzato per la raccolta di tutti gli eventi clinici legati al paziente (episodi, referti, esami, ecc.) in formato sia documentale sia strutturato, si propone la diffusione del Clinical Data Repository (CDR) aderente allo standard HL7 Fast Healthcare Interoperability Resource (FHIR) nel seguito denominato CDR-FHIR, rendendo disponibili tutte le Application Programming Interface (API). Sarà garantita l'alimentazione verso il CDR-FHIR:

- sia in maniera diretta da parte degli attuali applicativi Producer "FHIR ready" (conformi all'implementazione clinica delle strutture sanitarie della Regione Puglia);
- sia degli attuali applicativi conformi allo standard HL7 v2.x che effettuano accettazioni, ammissioni, trasferimenti, chiusure ma anche raccolta di dati clinici (es. CUP, PACS, RIS, LIS, ADT, PS, ecc.).

Il CDR-FHIR sarà implementato nel rispetto del DECRETO 20 maggio 2022 "Adozione delle Linee guida per l'attuazione del Fascicolo sanitario elettronico" (22A03961) (GU Serie Generale n.160 del 11-07-2022) e ne rappresenta una iniziativa futuribile per coprire il ruolo di punto unico di integrazione verso il FSE2.0.
Per la corretta archiviazione e consultazione dei dati tutti gli Event Source condivideranno gli stessi dizionari come ad esempio: reparti richiedenti, reparti eroganti e codici episodi, utilizzando come fonte le basi di dati già consolidate in Edotto (p.es. Anagrafe delle strutture sanitarie). Tali codifiche verranno condivise in fase di configurazione del sistema. La codifica degli episodi sarà resa univoca a livello aziendale per poter gestire le regole di accesso e di gestione della privacy.
La comunicazione prevista verso il CDR-FHIR sarà basata su standard FHIR HL7 versione R4b su protocollo HTTPS; inoltre, si pone particolare attenzione agli aspetti di sicurezza per le integrazioni fra i sistemi dipartimentali e il Clinical Data Repository per i messaggi basati su Web service SOAP, HL7 over HTTPS e HTTPS REST.

Architettura CDR-FHIR

Il CDR-FHIR sarà strutturato sui seguenti moduli:

- *Data Ingestion Service e Terminology Server*;
- *Database* FHIR dei dati Clinici;
- API *Server* FHIR;
- *Security & Privacy*;
- Integrazione Anagrafe Assistiti.

Data Ingestion Service e Terminology Server

Il Data Ingestion Service sarà un modulo costituito da un insieme di connettori, uno per ogni standard di messaggio in ingresso. Questa struttura a connettori rende facilmente estendibile il Data Ingestion Service a ricevere qualsiasi formato o standard di messaggio o documento contenente dati sanitari trasmesso con il relativo protocollo di comunicazione.
Ogni connettore provvederà alla decodifica del messaggio proveniente dai sistemi esterni codificati nello standard per cui lo specifico connettore è implementato: lo valida, ne allinea la terminologia ad un dizionario comune tramite l'uso delle codifiche del Terminology Server, lo trasforma in formato FHIR e lo deposita nel Database FHIR dei dati clinici.
Saranno disponibili i connettori per messaggi FHIR R4b, HL7 v2.x e documenti CDA-2 iniettato in PDF firmato PADES o XADES. Il servizio sopra descritto potrà essere attivato in maniera configurabile per permettere l'implementazione di tale modulo nel contesto del CDR-FHIR o in alternativa per delegare l'attività da esso svolta a componenti esterne (es. Gateway Nazionale).

FHIR Database Dati Clinici

Il modulo FHIR Database Dati Clinici costituirà il repository destinato a contenere le risorse memorizzate secondo lo standard FHIR ed estratte dai messaggi e dai documenti sanitari ricevuti sia tramite il Data Ingestion Service sia direttamente tramite il FHIR API Server.

FHIR API Server

Il modulo FHIR API Server renderà disponibili le risorse FHIR contenute nel FHIR Database Dati Clinici alle applicazioni che utilizzano lo standard di comunicazione FHIR R4b, inoltre potrà ricevere e conservare nel FHIR Database Dati Clinici i dati inviati da sistemi interni od esterni alla rete regionale che nativamente comunicano con lo standard FHIR e sono conformi alla strutturazione dei dati clinici di Regione Puglia.

Security & Privacy

Questo modulo avrà la responsabilità di gestire le policy di sicurezza per le applicazioni che si integrano direttamente sul FHIR API Server producendo o richiedendo le risorse contenenti dati sanitari contenuti nel CDR-FHIR, nonché mediare i consensi e autorizzazioni per la visualizzazione e l'utilizzo dei dati sanitari da parte dei consumer tramite l'integrazione con il sistema aziendale Gestore Consensi già previsto nel progetto CCE e indicato nel successivo paragrafo.

Integrazione Anagrafica Assistiti

A garanzia della corretta gestione del dato, tutti i producer di dati sanitari condivideranno la stessa anagrafe degli assistiti, quindi lo stesso identificativo univoco del paziente. Il CDR-FHIR accetterà alimentazioni solo se associati a un identificativo univoco del paziente verificabile puntualmente sull'Anagrafe Centrale tramite il modulo Integrazione Anagrafe Assistiti.

EVOLUZIONE DEL SISTEMA GESTIORE DEI CONSENSI

La componente aziendale di Gestione dei Consensi già sviluppata dovrà essere evoluta per consentire almeno, a titolo esemplificativo:

- la gestione degli oscuramenti/deoscuramenti direttamente su interfaccia grafica, ad uso di personale abilitato (p.es. medico che ha prodotto il documento o l'unità di rischio clinico aziendale)
- la gestione dei dati di contatto degli assistiti (p.es. numero di telefono, indirizzo e-mail) con gli opportuni meccanismi di certificazione dei contatti
- integrazione con sistemi (p.es. Portale della Salute della Regione Puglia, FSE) per la gestione, tramite servizi telematici, dei consensi (p.es. consenso all'utilizzo della firma grafometrica, consenso alla costituzione e alimentazione DSE anche con i dati pregressi, consenso all'utilizzo dei dati di contatto per specifiche finalità) direttamente da parte dell'assistito;
- eventuali migliorie sulla gestione del consenso informato al trattamento sanitario.
-

GESTIONE DEI BACKUP DELLE CARTELLE CLINICHE

Al fine di garantire la continuità operativa e la sicurezza delle informazioni contenute nella cartella clinica elettronica, è imprescindibile che l'offerente presenti un dettagliato piano di resilienza specifico per la gestione delle cartelle cliniche. Tale piano deve includere strategie comprovate per il backup periodico dei dati, la loro conservazione in ambienti sicuri e separati, e la rapida ripristinabilità in caso di eventi avversi quali guasti hardware, disastri naturali o attacchi informatici. Si richiede altresì che il piano preveda test regolari della procedura di ripristino, per assicurare l'efficacia e l'aggiornamento continuo delle misure di sicurezza adottate. Tutto ciò dovrà essere documentato e aggiornato periodicamente, in conformità con le normative vigenti sulla protezione dei dati personali e sulla sicurezza delle informazioni sanitarie.

Si chiede inoltre, di descrivere nel progetto tecnico il "Piano di backup" che deve includere almeno i seguenti paragrafi:

- Obiettivi del backup: Definizione degli obiettivi di protezione dei dati, come la disponibilità, l'integrità e la riservatezza.
- Frequenza dei backup: Determina con quale frequenza vengono eseguiti i backup dei dati. Può variare a seconda della criticità dei dati.
- Metodi di backup: Specifica quali metodi di backup saranno utilizzati, come backup completo, incrementale o differenziale.
- Strategia di archiviazione: Descrive dove verranno archiviati i backup, ad esempio su supporti fisici come dischi rigidi esterni o su cloud.
- Procedure di backup: Dettaglia le procedure specifiche per eseguire i backup, inclusi i passaggi da seguire e le risorse necessarie.
- Test di ripristino: Indica come e con quale frequenza verranno testate le procedure di ripristino per assicurarsi che i backup siano recuperabili in caso di necessità.
- Responsabilità: Specifica chi è responsabile dell'esecuzione dei backup, del monitoraggio e del ripristino dei dati in caso di perdita.
- Politiche di conservazione dei dati: Definisce per quanto tempo vengono conservati i backup prima di

essere eliminati o archiviati.
- Risorse necessarie: Elenco delle risorse hardware, software e umane necessarie per implementare il piano di backup.
- Procedure di emergenza: Include le procedure da seguire in caso di incidente che richieda il ripristino dei dati da backup.

Il progetto Tecnico deve prevedere un piano di continuità del business (BCP) per una cartella clinica elettronica al fine di garantire la disponibilità continua dei dati e la prestazione dei servizi sanitari anche in situazioni di emergenza o interruzioni critiche.

Il piano di BCP deve prevedere almeno i seguenti punti:

- Analisi dei rischi: analisi dettagliata dei potenziali rischi e delle minacce che potrebbero influenzare la disponibilità dei servizi della cartella clinica elettronica. Questi potrebbero includere guasti hardware, attacchi informatici, catastrofi naturali, interruzioni dei servizi di rete e altro ancora.
- Identificazione delle priorità e dei servizi essenziali: Identificare i servizi sanitari critici supportati dalla cartella clinica elettronica e stabilire le priorità per il ripristino in caso di interruzione. Questo potrebbe includere l'accesso ai dati dei pazienti, la prescrizione elettronica, la gestione degli appuntamenti e altri servizi fondamentali.
- Pianificazione di emergenza: Sviluppare procedure dettagliate e protocolli operativi da seguire in caso di emergenza. Questo potrebbe includere la designazione di un team di risposta alle emergenze, la definizione di ruoli e responsabilità del personale, nonché le procedure per la comunicazione interna ed esterna durante un'interruzione.
  Infrastruttura tecnologica resiliente: l'infrastruttura tecnologica deve supportare la continuità operativa, includendo la ridondanza dei server critici, la distribuzione dei dati e delle servizi applicativi per garamtire una protezione avanzata sia contro le minacce informatiche che in caso di guasti hardware

Con riferimento a quest'ultimo punto nel piano di continuità del business si potrà fare riferimento a risorse da dislocare presso le singole strutture ospedaliere.

SOLUZIONE EVOLUTIVA DEL MODULO DI SOMMINISTRAZIONE TERAPIA

Il modulo di prescrizione terapia, già presente in CCE , dovrà evolvere per eseguire dei controlli e restituire informazioni per migliorare la sicurezza del paziente e l'appropriatezza della somministrazione. In particolare dovrà almento:

- Eseguire controlli automatici su eventuali reazioni avverse/allergie del paziente, segnalate nell'apposita procedura di prima valutazione, anche ad uno solo dei principi attivi selezionati dal medico e avvisare attraverso degli alert il rischio di evento avverso, tracciando l'informazione qualora il medico confermasse la sua selezione dopo l'avviso;
- Essere fornito di controlli automatici (abilitabili singolarmente) per i seguenti valori:
  - Doppie prescrizioni per il medesimo paziente;
  - Allergie (sulla base del principio attivo presente all'ultimo livello della codifica ATC);
  - Dosaggi impropri;
  - Interazioni tra farmaci prescritti;
  - Via di somministrazione per farmaco prescritto
- disporre di funzionalità di supporto clinico decisionale che, sulla base dei dati presenti nella CCE del paziente, forniscano in modalita automatica informazioni rilevanti per il caso clinico specifico, suggerimenti sulla prosecuzione del percorso clinico, messaggi e avvisi di possibili situazioni critiche e allarmi oltre ad altre informazioni potenzialmente utili per la gestione efficace e sicura dello specifico processo clinico.

Si richiede inoltre di implementare in CCE le funzionalità di collegamento con l'armadietto di reparto per rendere le richieste d'acquisto e le successive evasioni d'ordine coerenti con il livello di produzione ospedaliera, i livelli di giacenza nei magazzini (sia centrale che di reparto), con i tempi di consegna dei fornitori e con la stagionalità dei consumi.

In particolare da CCE l'operatore dovrà poter visionare le scorte dell'armadietto di reparto (alimentato e

aggiornato dal sistema amministrativo contabile unico regionale) e monitorare la dinamica di "svuotamento" dell'armadietto che avviene a seguito della prescrizione effettuata in CCE e del prelievo dall'armardietto di reparto e alla somministrazione della terapia. Il cruscotto in CCE deve poter visualizzare gli articoli forniti dal sistema di magazzino e quelli effettivamente utilizzati durante l'assistenza clinica.

Inoltre, per diminuire i rischi associati alla mancanza di farmaci essenziali e ridurre il carico amministrativo del reparto, il sistema deve essere dotato di un meccanismo di gestione automatizzata degli ordini che, al raggiungimento di una soglia predefinita minima definita, innesca automaticamente la richiesta di rifornimento per i farmaci in esaurimento.

SOLUZIONE EVOLUTIVA DELLA CARTELLA CLINICA ELETTRONICA PER LA GESTIONE DELLA CARTELLA DI SALUTE MENTALE

L'obiettivo è avere una CCE che deve essere verticalizzata e configurata per soddisfare le esigenze dei Servizi di Salute Mentale riportando le funzionalità previste attualmente e riutilizzando, per quanto possibile, le funzionalità e i servizi esistenti.
Il Sistema Informativo nazionale per il monitoraggio e tutela della Salute Mentale (SISM), è stato realizzato per monitorare gli interventi sanitari erogati alle **persone adulte con problemi psichiatrici** ed alle loro famiglie; resta esclusa, pertanto, la Neuropsichiatria infantile.
Il flusso di alimentazione è regolamentato dal DM 15 ottobre 2010 del Ministero della Salute.
Il DM 15/10/2010 dispone che il conferimento dei dati da parte delle Regioni, a partire dal 1° gennaio 2012, è adempimento per l'accesso al finanziamento integrativo a carico dello Stato, ai sensi dell'Intesa sancita dalla Conferenza Stato-Regioni il 23/3/2005.
Al fine di soddisfare gli obblighi informativi verso il Ministero della Salute e di fornire agli operatore dei Dipartimenti di Salute Mentale delle ASL pugliesi uno strumento di monitoraggio dell'assistenza erogata, la Regione Puglia si è dotata, per il tramite di InnovaPuglia S.p.A. di un sistema informativo regionale della salute mentale, denominato **DISAMWEB.**
Con Determina Dirigenziale 081/2024/47 del 12/03/2024 si è provveduto all'affidamento (CIG B0BE679901) per un periodo di 24 mesi dei servizi di Gestione applicativa e supporto utenti, Manutenzione adeguativa e correttiva e Conduzione tecnica infrastruttura; la scadenza naturale del contratto è fissata al 12/03/2026; entro quella data si dovrà procedere alla migrazione delle funzionalità previste all'interno della CCE.
La documentazione tecnica verrà fornita all'aggiudicatario dopo la stipula del contratto.

SOLUZIONE EVOLUTIVA DELLA CARTELLA CLINICA ELETTRONICA PER LA GESTIONE DELLA INFORMAZIONI RELATIVE ALLE DIPENDENZE PATOLOGICHE

L'obiettivo è avere una CCE che deve essere verticalizzata e configurata per soddisfare le esigenze dei DipartimentI delle Dipendenze Patologiche e dei SerT riportando le funzionalità previste attualmente e riutilizzando, per quanto possibile, le funzionalità e i servizi esistenti.
Ai fini del monitoraggio delle attività dei Dipartimenti delle Dipendenze Patologiche e dei SerT, la Regione Puglia dispone da diversi anni di un proprio sistema informativo regionale, aggiornato da novembre 2013 a seguito di concessione in riuso da parte della Azienda USL Pisa 5 del sistema HTH - Ascolta la Salute (modulo dipendenze).
Attraverso il sistema regionale si procede inoltre al soddisfacimento degli obblighi informativi verso il Ministero della Salute.
Con Determina Dirigenziale 081/2024/25 del 27/02/2024 si è provveduto all'affidamento per un periodo di 24 mesi dei servizi di Gestione applicativa e supporto utenti, Manutenzione adeguativa, Assistenza da remoto e specialistica e correttiva e Conduzione tecnica infrastruttura; la scadenza naturale del contratto è fissata al 28/02/2026; entro quella data si dovrà procedere alla migrazione delle funzionalità previste all'interno della CCE.
La documentazione tecnica verrà fornita all'aggiudicatario dopo la stipula del contratto.

SOLUZIONE EVOLUTIVA DELLA CARTELLA CLINICA ELETTRONICA PER GLI OSPEDALI DI COMUNITÀ E CASE DELLA COMUNITÁ

La CCE deve poter essere verticalizzata e configurata per soddisfare le esigenze degli Ospedali di Comunità e delle Case della Comunità riutilizzando per quanto possibile le funzionalità e i servizi esistenti. Attraverso l'applicativo

di CCE deve essere possibile gestire la raccolta e l'invio delle informazioni a Edotto propedeutiche all'invio del nuovo flusso individuato nel PNRR Missione 6 Componente 2 relativo agli Ospedali di Comunità.

Si precisa che nell'ambito del progetto verranno definite le specifiche, attualmente in corso di definizione, affinchè la CCE venga utilizzata anche per la gestione degli Ospedali di Comunità e Case della Comunità.

INTEGRAZIONE CON LA CENTRALE OPERATIVA TERRITORIALE(COT)

Il DM77/2022 introduce la Centrale Operativa Territoriale (COT) come un modello organizzativo che svolge una funzione di coordinamento della presa in carico della persona e raccordo tra servizi e professionisti coinvolti nei diversi setting assistenziali: attività territoriali, sanitarie e sociosanitarie, ospedaliere e dialoga con la rete dell'emergenza-urgenza.). Tra le funzioni della COT vi è la gestione delle transizioni dei pazienti tra setting diversi e opera come vettore di coordinamento e raccordo tra i nodi e i professionisti dei diversi setting (ospedaliero, territoriale).

La COT assolve al suo ruolo di raccordo tra i vari servizi attraverso funzioni distinte e specifiche, seppur tra loro interdipendenti:

- coordinamento della presa in carico della persona tra i servizi e i professionisti sanitari coinvolti nei diversi setting assistenziali (transizione tra i diversi setting: ammissione/dimissione nelle strutture ospedaliere, ammissione/dimissione trattamento temporaneo e/o definitivo residenziale, ammissione/dimissione presso le strutture di ricovero intermedie o dimissione domiciliare);
- coordinamento/ottimizzazione degli interventi, attivando soggetti e risorse della rete assistenziale;
- tracciamento e monitoraggio delle transizioni da un luogo di cura all'altro o da un livello clinico assistenziale all'altro;
- supporto informativo e logistico, ai professionisti della rete assistenziale (MMG, PLS, MCA, IFeC ecc.), riguardo le attività e servizi distrettuali;
- raccolta, gestione e monitoraggio dei dati di salute, anche attraverso strumenti di telemedicina, dei percorsi integrati di cronicità' (PIC), anche attraverso strumenti di telemedicina, dei pazienti in assistenza domiciliare e gestione della piattaforma tecnologica di supporto per la presa in carico della persona (telemedicina, teleassistenza, strumenti di e-health, ecc.)

Per assolvere al suo ruolo, la COT deve ricevere e dare informazioni alla CCE relativamente a titolo esemplificativo alla disponibilità di posti letto dei presidi ospedalieri e ai cambi di stato relativi ai pazienti registrati in CCE (es. cambio stato da ricoverato a dimesso).

Si precisa che nell'ambito del progetto verranno definite le specifiche, attualmente in corso di definizione, affinché la CCE si integri opportunamente con le Centrali Operative Territoriali.

L'integrazione dlla CCE con le COT deve consentire la compilazione della scheda di valutazione multidisciplinare che sarà prevista dal a livello regionale oltre alla possibilità di compilare ulteriori schede di valutazionoe multidisciplinare a livello aziendale.

La scheda compilata nell'ambito della CCE verrà inviata, nei suoi contenuti strutturati, alla COT che provvederà a metterla a disposizione della componente di Assistenza Domiciliare di Edotto attraverso specifico servizio.

SVILUPPO INTEGRAZIONI CON ALTRI SISTEMI

La Cartella Clinica Elettronica deve consentire l'interoperabilità applicativa con i sistemi attualmente presenti in Regione Puglia o in corso di sviluppo, per lo scambio reciproco delle informazioni, grazie alla condivisione di dati strutturati e non, tramite cooperazione secondo standard FHIR o tramite opportuni sviluppi di API per abilitare ad esempio il colloquio bidirezionale con la Data Platform Regionale. Il Repository FHIR, componente centrale e fondamentale dell'architettura, permetterà di creare un punto unico e centralizzato per l'interscambio delle informazioni tra le varie componenti applicative presenti in Regione Puglia [Non emerge la relazione tra il Repository FHIR e il Repository XDS di CCE].

La Cartella Clinica Elettronica deve condividere i dati raccolti puntualmente e in conformità alle disposizioni normative vigenti in tema di protezione dei dati personali, permettendo a chi autorizzato e interessato di essere

informato della presenza di nuove informazioni e al tempo stesso di generare flussi informativi disaccoppiati di comunicazione verso sistemi esterni.
Questo processo di evoluzione architetturale e tecnologica permetterà un disaccoppiamento tra i componenti, con un punto unico di accesso e recupero del dato in *near real-time*, semplificando l'interazione tra i sistemi e lo scambio di informazioni comuni, evitando la duplicazione del dato e possibili incoerenze.

Di seguito l'elenco non esaustivo dei sistemi con cui si richiede l'interfacciamento al fine di mettere a fattor comune i dati raccolti dai sistemi per permettere una gestione integrata e completa delle informazioni del paziente.

Si precisa che nell'ambito di validità del presente progetto, laddove non fosse ancora definito il servizio regionale destinatario dell'attività richiesta, si prevede che sia oggetto di richiesta specifica successiva nelle forme previste dal CTS Lotti Applicativi nel corso del progetto.

Integrazioni per la prescrizione del primo ciclo di cura

Il Sistema deve consentire tramite la componente di prescrizione dematerializzata la prescrizione del primo ciclo di cura alla dimissione, integrandosi opportunamente con la farmacia ospedaliera o con il MOSS.

Integrazione con il sistema regionale di gestione del paziente renale

L'applicativo di CCE regionale deve evolversi per integrarsi con il sistema informativo regionale di Gestione del Paziente Renale al fine di, a titolo esemplificativo:

- consentire agli operatori ospedalieri e ambulatoriali di utilizzare un unico applicativo che soddisfi le specificità della specialità clinica;
- garantire l'alimentazione della piattaforma regionale per la gestione del paziente renale con i dati di interesse registrati nell'applicativo CCE (p.e. dati necessari per la gestione del percorso di dialisi , dati finalizzati alla gestione dei trapianti);
- permettere la condivisione in tempo reale dei dati dei ricoveri in caso di trasferimenti da e verso i reparti di nefrologia.

Integrazione con il sistema delle liste di attesa dei trapianti

L'applicativo di CCE deve notificare al sistema informativo che gestisce le liste di attesa per i trapianti utilizzato dal Centro Regionale di Riferimento dei trapianti, la presunta futura disponibilità di un donatore (morte encefalica) sia dall'area Pronto Soccorso che dai reparti (p.es. terapia intensiva) corredando la notifica con tutte le informazioni necessarie, nonché la notifica della effettiva disponibilità del donatore.
Integrazione con il Sistema applicativo di gestione delle reti tempodipendentiL'applicativo di CCE regionale deve evolversi per integrarsi con il sistema informativo regionale di Gestione delle Reti T-Dipendenti al fine di, a titolo esemplificativo:

- consentire agli operatori ospedalieri di utilizzare un'unica piattaforma applicativa per condividere dati e funzionalità;
- garantire l'alimentazione della piattaforma regionale con i dati di interesse registrati nell'applicativo CCE;
- permettere la condivisione dei dati registrati nella piattaforma regionale in caso di ricovero.

Integrazione con il Sistema Trasfusionale Regionale "EMOPUGLIA"

L'applicativo di CCE regionale, attraverso la componente di Order Entry già disponibile, deve essere in grado di effettuare le richieste di emoderivati verso il Sistema Informativo Trasfusionale regionale. Devono essere gestiti tutti i flussi operativi nonché le notifiche di cambio stato dall'invio della richiesta alla presa in carico fino alla consegna. Deve inoltre essere gestito tutto il processo di associazione sacca/paziente attraverso opportuni meccanismi di identificazione.

Integrazione con il Sistema di BI Regionale

Nell'ambito dell'OR _1 Big Data, Open Data, i (DSS), del *Citizen Relationship Management* (CRM) Piano Triennale di riorganizzazione digitale è stato affidato a InnovaPuglia la messa in produzione del DSS CRM, struttura per la

gestione di Big Data che mette a disposizione servizi per l'Analisi e BI.

Il progetto prevede due macro-componenti:

- Il datawarehouse open source che prevederà la collezione di tutti i dati da tutti i sistemi informativi regionali DSS;
- CRM: si basa sui dati DSS per approfondire la *Citizen experience*. Il sistema sarà bidirezionale e anche il cittadino potrà consultare dati.

L'interazione degli applicativi con la BI si baserà sulle seguenti opzioni:

- Alimentazione del sistema BI/DSS per fornire i dati su cui fare le integrazioni, tramite connettore o API;
- Acquisizione dei dati del DSS per la fruizione di tali dati attraverso un sistema di reportistica;
- Possibilità di fare all'interno del DSS delle verticalizzazioni contenutistiche

La CCE regionale deve poter alimentare con dati opportunamente pseudoanonimizzati il sistema di BI attraverso opportuni connettori per poter dialogare con il DSS e deve prevedere un'interfaccia con il sistema di DSS per poter alimentare il sistema di reporting. Questa interazione deve essere bidirezionale.
Le specifiche di trasferimento dei dati dall'applicativo di CCE e il sistema di BI regionale saranno successivamente concordate.

Integrazione con il sistema di telemedicina regionale di-Televisita

L'applicativo di Cartella Clinica Elettronica, deve essere esteso per poter gestire anche i pazienti tramite televisita mediante integrazione della piattaforma di telemedicina individuata dalla Regione Puglia.

Integrazione con i monitor per la gestione dei parametri vitali

Il progetto evolutivo prevede l'implementazione delle funzionalità necessarie a gestire gli automatismi di trasferimento e gestione (in *real time*) in Cartella Clinica Elettronica dei parametri vitali dai monitor permettendo risparmi di tempo e aumentando la produttività del personale. In questo modo i medici possono valutare lo stato di salute del paziente da remoto consultando dati sempre recenti.

Integrazione con i dispositivi di emogasanalisi

L'applicativo di CCE deve essere integrato con i dispositivi di Emogasanalisi per ottenere direttamente in CCE sia il referto prodotto che i dati strutturati attinenti ai singoli valori derivanti dal referto prodotto.

Integrazione con l'applicativo per la Gestione dei Pasti

L'applicativo di Cartella Clinica Elettronica consente al medico di definire la tipologia di dieta da associare al paziente; attraverso specifici servizi di cooperazione deve inviare al sistema di gestione pasti, se disponibile, la tipologia di dieta al fine di predisporre il pasto corrispondente.

Integrazione con Edotto per la gestione dei flussi

L'integrazione tra l'applicativo di CCE regionale e il sistema Edotto garantirà almeno i seguenti flussi informativi:

- EMUR: Il modulo di Pronto Soccorso provvede a produrre il contenuto informativo relativo al flusso in questione e dispone delle funzionalità necessarie all'invio alla componente dei Flussi Informativi di Edotto (GAF) che provvede alla gestione delle trasmissioni al Ministero
- Schede Implantologiche: la Cartella Clinica Elettronica, attraverso la componente di Sale Operatorie provvede a gestire i dati necessari a produrre il contenuto informativo; la stessa componente consente, tramite funzionalità specifica, l'invio a Edotto per gli adempimenti necessari.
- Schede di morte: la Cartella Clinica Elettronica alla dimissione del paziente deve gestire le informazioni necessarie ad alimentare il contenuto informativo del Registro Mortalità di Edotto; la cartella di reparto, tramite funzionalità specifica, invia a Edotto il flusso in questione per gli adempimenti necessari. Inoltre, l'applicativo di CCE deve consentire la compilazione della documentazione necessaria in caso di dimissione per decesso.
- CEDAP: la Cartella Clinica Elettronica nella sua verticalizzazione di Ginecologia e Ostetricia provvede a gestire le informazioni necessarie a produrre il Certificato di Assistenza al Parto i Modelli ISTAT D.11 e

D.12 relativi rispettivamente all'Aborto Spontaneo e all'Interruzione Volontaria di Gravidanza. Il certificato e i dati dei modelli ISTAT vengono comunicati a Edotto per la parte di gestione del l'area di competenza. Sarà necessario eventualmente integrare la verticalizzazione di ginecologia/ostetricia per i dati relativi all'IVG e aborto spontaneo.

Integrazione CCE/FSE in lettura

L'attuale implementazione dell' integrazione tra la Cartella Clinica Elettronica e il Fascicolo Sanitario Elettronico prevede che Repository Documentale Aziendale alimenti il FSE (istituito dalla Regione Puglia ai sensi dell'art.12 della L. 17 dicembre 2012, n. 221, di conversione del D.L. 18 ottobre 2012, n. 179) con documenti strutturati secondo lo standard HL7 CDA r2 rispondenti al modello FSE 2.0 (cioè documenti in formato pdf, firmati digitalmente in PADES e aventi i dati strutturati CDA iniettati nel medesimo pdf). L'integrazione innanzi descritta sarà ampliata ed evoluta per mettere a disposizione degli operatori sanitari, utenti di CCE, nuove funzionalità volte a semplificare e velocizzare l'accesso ai documenti clinici indicizzati nel FSE in modo da presentare, i dati e i documenti, in modalità efficace e navigabile con lo scopo di garantire una maggiore circolarità delle informazioni cliniche di un assistito.

Si rende quindi necessario consolidare, efficientare e potenziare i servizi esistenti di alimentazione del FSE (alimentazione in tempo reale direttamente dal Repository Clinico Aziendale e non mediato da terze componenti infrastrutturali -framework-) e, contestualmente, implementarne di nuovi, a valore aggiunto per gli operatori sanitari, che consentano la consultazione organizzata dei documenti in modo da rendere il FSE un reale punto di riferimento per la storia clinica del paziente durante i percorsi sia di ricovero che ambulatoriali.

L'integrazione, oltre alla possibilità di ricercare e consultare i documenti clinici riferiti agli assistiti di competenza, deve consentire ai professionisti sanitari, utenti di CCE, di poter arricchire la loro visione globale sullo stato di salute del paziente sulla base del patrimonio informativo offerto dal FSE.

Infatti, al fine di mettere in evidenza la cronologia degli eventi clinici e dei dati e documenti ad essi connessi, la CCE dovrà rappresentare in forma grafica, e in linea temporale, una sintesi degli eventi e dei dati (indicizzati in FSE) offrendo la possibilità di navigazione tra le diverse dimensioni informative anche su scale temporali diverse, scelte dinamicamente dall'utente operatore sanitario.

Integrazione col registro RIPO

L'articolo 40 della L.r. n.4 del 25 febbraio 2010 ha istituito il Registro Regionale di Implantologia Protesica della Regione Puglia, disponendo che tutti i soggetti erogatori di prestazioni di ricovero ospedaliero, pubblici ed accreditati, in cui vengono effettuati interventi di implantologia protesica di anca e/o di ginocchio, sono tenuti a compilare una apposita scheda. Obiettivo principale della costruzione del Registro nazionale di protesi d'anca è quello di creare un livello base di informazioni disponibili: un vero e proprio censimento di tutto ciò che viene impiantato (informazioni sul paziente, sull'intervento e sul dispositivo impiantato). A partire da queste informazioni è possibile effettuare analisi di sopravvivenza degli impianti e garantire la rintracciabilità dei pazienti nel caso di problemi.

Il RIPO, infatti, è in grado di identificare in tempo reale i pazienti cui fosse stata impiantata una protesi articolare che, in base a recall effettuati dal Ministero della Salute o dalle ditte produttrici, dovesse essere considerata a rischio di fallimento precoce. In tale evenienza i chirurghi ortopedici possono essere messi in condizione di attivare prontamente tutte le misure necessarie per la tutela della salute del paziente.

Ai chirurghi viene richiesto attraverso un apposito modulo di fornire alcune informazioni e applicare l'etichetta dei singoli componenti delle protesi impiantate ai pazienti. Il personale del RIPO provvede alla validazione dei dati e all'inserimento in banca dati, nonché all'esecuzione delle analisi statistiche sui dati stessi.

I dati raccolti in CCE dovranno essere integrati per alimentare il registro RIPO, ad esempio mediante flussi o *webservices* e occorrerà acquisire l'etichetta dei singoli componenti delle protesi impiantate ai pazienti.

Integrazione con il sistema di conservazione regionale

I documenti sanitari prodotti con l'applicativo di CCE regionale, nonché tutti i documenti sanitari inviati al Repository Clinico Aziendale, devono essere trasmessi al sistema di conservazione regionale. È necessario, pertanto integrarsi con i servizi esposti dal suddetto sistema di conservazione, previa definizione dei processi e dei ruoli e responsabilità coinvolte.

Integrazione con il MOSS

Il sistema deve integrarsi con il sistema MOSS per rendere le richieste d'acquisto e le successive evasioni d'ordine coerenti con il livello di produzione, i livelli di giacenza nei magazzini (sia centrale che di reparto), con i tempi di consegna dei fornitori e con la stagionalità dei consumi.

Integrazione con il SIST

Si chiede l'evoluzione dell'integrazione del sistema di *e-prescription* con il SIST oggi effettuata tramite chiamata di contesto al fine di ottimizzare la comunicazione e cooperazione tra gli applicativi.

Integrazione con il CUP

Si chiede di implementare una soluzione che consenta la gestione delle prenotazioni da parte dell'ambulatorio verso il CUP che non sia relativa esclusivamente all'ambulatorio di afferenza.

ULTERIORI SERVIZI EVOLUTIVI

Nel corso del contratto, l'Amministrazione potrà richiedere ulteriori interventi evolutivi con l'obiettivo di adeguare l'infrastruttura applicativa a nuove esigenze funzionali che potranno manifestarsi attraverso la creazione di nuove funzionalità degli applicativi esistenti, creazione di nuovi moduli o re-engineering di funzionalità esistenti o dell'architettura applicativa del sistema.
Per ciascun intervento richiesto dovrà essere effettuata una analisi tecnica di fattibilità con valutazione dell'effort in giorni/persona necessario e la definizione dei tempi di realizzazione, da sottoporre all'approvazione del Committente.

Tra la documentazione da fornire rientra anche la produzione della documentazione e dei WBT (Web-Base-Training) che verranno conocordati con l'Amministrazione rappresentanti le evoluzioni delle funzionalità di CCE e che dovranno essere messi a disposizione per essere integrati nella piattaforma di e-learning regionale / aziendale.

Configurazione e Personalizzazione di Soluzioni di terze parti/open source/riuso (PP)

In questo servizio sono compresi interventi di configurazione della piattaforma di CCE utilizzando funzionalità già previste perché già realizzate e/o che saranno oggetto di evoluzione o nuovo sviluppo.

In particolare rientrano in questo servizio le attività previste dal Capitolato Tecnico Speciale:

- utilizzo di tabelle standard, accessibili tramite menù decodificati, in cui è possibile definire il funzionamento del programma/pacchetto/software in uso, normalmente senza necessità di scrittura di codice sorgente.
- realizzazione di ulteriori moduli software su richiesta dell'Amministrazione, per soddisfare requisiti non originariamente presenti nella soluzione software adottata o non risolvibili con soli interventi di parametrizzazione.
- determinazione delle caratteristiche necessarie alla messa a punto del software affinché risulti correttamente installato e garantisca, mediante l'attivazione dei moduli disponibili e/o di dotazioni opzionali, la copertura funzionale e non attraverso la parametrizzazione di funzionalità native in cui è possibile impostare determinati parametri e/o definire il funzionamento desiderato;
- copertura di ulteriori esigenze funzionali non originariamente offerte dalla soluzione con una limitata attività di sviluppo software, come per esempio la predisposizione di interfacce con altri sistemi, la realizzazione di funzionalità non presenti nel pacchetto/sw esistente, nuovi rapporti di stampa, o altro.

Per lo svolgimento delle attività, si richiede la disponibilità di personale dedicato alle attività di parametrizzazione e personalizzazione che provveda, inoltre, alle attività di seguito indicate a livello esemplificativo e non esaustivo

- modifiche di parametri di esecuzione o di tabelle di riferimento o decodifica;
- attività di parametrizzazione specifiche su procedure, parametri e tabelle, manuale utente, manuale di gestione, definizioni relative ai dati, ecc.;
- gestione della nuova configurazione.

Il personale dedicato a questo servizio dovrà, inoltre, predisporre il giornale delle configurazioni e personalizzazioni con indicazione del richiedente, della data di inizio e della data di fine delle attività oltre alla risorsa che ha concluso l'attività.

Manutenzione Adeguativa, Migliorativa e Correttiva (MAD-MAC)

Il servizio di Manutenzione Adeguativa e Migliorativa comprende l'attività volta ad assicurare la costante aderenza delle procedure e dei programmi
all'evoluzione dell'ambiente tecnologico del sistema informativo. Comprende tutti gli interventi sul software che non rientrano nella correttiva e nella evolutiva, conseguenti a cambiamento dei requisiti (organizzativi, normativi, d'ambiente, di prodotto-tecnologia-ambienti-piattaforma) che non richiedano una variazione dei requisiti funzionali.
Il servizio, relativamente anche a tutte le componenti già in esercizio per esempio di CCE (di ricovero ed ambulatoriale), Order Manager, Repository Clinico Aziendale, Blocco Operatorio, Gestore Consensi, e-prescription nonché alle integrazioni delle suddette applicazioni con altri sistemi informativi terzi, comprende le attività volte ad assicurare la costante aderenza delle procedure e dei programmi all'evoluzione dell'ambiente tecnologico del sistema informativo e al cambiamento di requisiti non funzionali.
Nella fattispecie il servizio potrà essere innescato dall'esigenze di:

- adeguamenti dovuti a cambiamenti di condizioni al contorno
- adeguamenti necessari per innalzamento di versioni del container, del software base e middleware
- adeguamenti tesi all'introduzione di nuovi prodotti o modalità di gestione del sistema
- modifiche, anche massive, non a carattere funzionale, alle applicazioni
- adeguamenti finalizzati a migliorare l'interoperabilità, l'integrazione e lo scambio dei dati
- adeguamenti finalizzati a migliorare le standardizzazione delle informazioni
- miglioramento dell'accessibilità e usabilità delle applicazioni
- ottimizzazione delle prestazioni di caricamento delle basi informative
- modifiche alle applicazioni, anche massive, di carattere non funzionale

Per quanto attiene ai requisiti e modalità di erogazione del servizio, al team di lavoro e alle metriche di dimensionamento si rimanda a quanto presente nel CTS Lotti applicativi al capitolo 4 relativamente al servizio oggetto del presente paragrafo.

Il servizio di Manutenzione Correttiva comprende le attività volte ad assicurare il corretto funzionamento delle applicazioni mediante la diagnosi e la rimozione delle cause e degli effetti, sia sulle interfacce utente che sulle basi dati che sulla documentazione, dei malfunzionamenti del software in esercizio.
Nella fattispecie il servizio dovrà garantire le seguenti attività di cui viene fornito elenco non esaustivo:

- Gestione di ticket per malfunzionamenti delle applicazioni nel perimetro, comprese le applicazioni già in esercizio quali ad esempio CCE (di ricovero ed ambulatoriale) Order Manager, Repository Clinico Aziendale, Blocco Operatorio, Gestore Consensi, e-prescription nonché le integrazioni delle suddette applicazioni con altri sistemi informativi terzi;
- contributi di competenza sistemistica e specialistica di prodotto necessari alla corretta soluzione del malfunzionamento;
- attivazione del gruppo di sviluppo per la risoluzione dei malfunzionamenti per adeguare l'eventuale software in corso di sviluppo/modifica/collaudo
- sviluppi necessari per la risoluzione dei malfunzionamenti;
- verifiche e collaudo delle modifiche prima del rilascio in produzione;
- test in apposito ambiente di sviluppo assimilabile all'ambiente di esercizio della soluzione realizzata;
- eventuale aggiornamento della documentazione tecnica e dei manuali utente e allineamento della documentazione.

Per quanto attiene ai requisiti e modalità di erogazione del servizio, al team di lavoro e alle metriche di dimensionamento si rimanda a quanto presente nel CTS Lotti applicativi al capitolo 4 relativamente al servizio oggetto del presente paragrafo.

Servizi di gestione applicativi e basi dati (GAB)

Per tutte le componenti già sviluppate nell'ambito del progetto CCE regionale (CCE di ricovero e ambulatoriale, Repository Clinico Aziendale, Gestore Consensi, Blocco Operariguardantorio, Order Manager, prescrizione dematerializzata) nonché per le nuove componenti/funzionalità oggetto del presente capitolato tecnico e per tutti gli Enti rientranti nel perimetro progettuale regionale e per quelli che rientreranno (es. ASL Foggia), deve essere garantito il Servizio di Gestione applicativa e basi dati che comprende le attività di governo, gestione e supporto per garantire l'operatività della piattaforma: gestione operativa dei caricamenti dei dati, monitoraggio e ottimizzazione delle prestazioni relativamente alle applicazioni, sincronizzazione delle applicazioni, validazione tecnica e controllo dei risultati delle elaborazioni e dei flussi informativi, pianificazione ed esecuzione di procedure e operazioni di ripristino, monitoraggio delle performance del sistema anche in termini di tempio di risposta degli applicativi.
Nella fattispecie il servizio si declinerà nelle seguenti attività:

- Gestione delle funzionalità in esercizio, tra cui a titolo esemplificativo si citano:
  - risoluzione delle richieste di intervento aperte all'utente;
  - validazione tecnica e controllo dei risultati delle elaborazioni, al fine di assicurare l'integrità e la correttezza dei dati presenti sulla base informativa, del contenuto dei flussi informativi provenienti o destinati ad organismi esterni e dei dati esposti negli elaborati del sistema;
  - ripristino base dati (non determinata da malfunzionamenti di software in garanzia od in manutenzione correttiva);
  - verifica ed aggiornamento di eventuale documentazione specifica della gestione applicativa
  - contenente FAQ, modi d'uso, modalità di esecuzione di particolari attività del servizio di gestione quali la manutenzione preventiva
  - predisposizione dell'ambiente dimostrativo (es. base dati, utenze specifiche, ecc).

- Presa in carico di nuove funzionalità in esercizio, tra cui a titolo esemplificativo si citano:
  - schedulazione e pianificazione del rilascio in esercizio di nuove funzionalità;
  - supporto alla predisposizione dell'ambiente di esercizio, e quanto necessario a consentire l'inizio delle attività da parte degli utenti;
  - affiancamento all'utente finale volto ad istruirlo all'uso delle funzionalità sia nuove che già presenti in esercizio
- Supporto agli utenti, per l'uso appropriato delle funzioni secondo le modalità previste nei manuali d'uso attraverso, a titolo esemplificativo:
  - assistenza tecnico/funzionale agli utenti;
  - preparazione di documentazione aggiuntiva rispetto a quella a corredo dei sistemi in esercizio (es. WBT), (es. documenti di sintesi, demo, presentazioni, ecc.);
- Pianificazione funzionale del servizio, tra cui a titolo esemplificativo:
  - movimentazione giornaliera dei batch, se applicabile;
  - disponibilità del servizio on line;
  - pianificazione ed esecuzione di elaborazioni di prova, con relativa ripresa di dati reali, a scopo di
  - manutenzione preventiva, per anticipare l'esito dell'elaborazione di procedure critiche per
  - l'Amministrazione.
  - Affiancamento per il trasferimento di *know how* necessario al corretto svolgimento del servizio:
  - l'attività consiste in una fase di "training on the job" a terzi individuati dall'Amministrazione,
  - finalizzata a trasmettere il *know how* funzionale applicativo e tecnico-sistemistico necessario alla
  - gestione del software in esercizio;
  - Attività di data entry e di archiviazione: finalizzata all'alimentazione iniziale o al recupero di dati/documenti o attività di supporto alle migrazioni e/o all'archiviazione digitale dei documenti

Di seguito vengono precisati i requisiti minimi richiesti dall'Amministrazione relativamente al supporto da remoto e on-site richiesto al Fornitore.

Affiancamento, monitoraggio adozione del sistema da parte degli utenti e supporto tecnico/funzionale e training on the job

Dovrà essere garantito il servizio di affiancamento all'utente finale volto a istruirlo sull'uso delle funzionalità sia in

uso che esistenti anche per il tramite delle seguenti attività:

- Affiancamento secondo la metodologia formativa del *training on the job,* relativamente a tutte le componenti già sviluppate nell'abito del progetto CCE, dei punti di erogazione dove la CCE non è stata ancora dispiegata e in particolare i presidi già esistenti (es. ASL Foggia) o in fase di completamento (es. Monopoli - Fasano) ;
- affiancamento del personale preposto all'utilizzo delle applicazioni oggetto di fornitura, secondo la metodologia formativa del *training on the job*. Tali moduli avranno lo scopo di completare e consolidare sul campo le competenze acquisite durante i corsi, operando in un ambiente reale di affiancamento al personale durante le attività operative. Le attività di affiancamento hanno lo scopo di:
  - assistere i discenti, garantendo ove richiesto la necessaria assistenza operativa per la risoluzione dei problemi connessi all'utilizzo quotidiano degli strumenti informatici e contribuendo alla risoluzione di dubbi o modalità operative improprie;
  - consolidare le abilità e le conoscenze acquisite durante l'addestramento online, necessarie per assolvere al meglio i propri compiti lavorativi, accrescendo padronanza e sicurezza nell'utilizzo del sistema;
  - garantire l'assistenza sul campo organizzando le attività in modo da coprire tutti gli utenti da affiancare sulla base dei loro turni e per un numero di giorni congruo a rendere gli utenti autonomi e sicuri;
- Monitoraggio dell'utilizzo della CCE e delle singole funzionalità e individuazione periodica (almeno bi-settimanale) delle criticità in termini di adozione;
- assistenza *on site* che consiste a titolo esemplificativo le seguenti tipologie di attività:
  - risorsa disponibile sul campo per rispondere alle richieste informative degli utenti, supportarne l'operatività, contribuire a rendere autonomi gli utenti, con riferimento a tutte le componenti sviluppate nell'ambito del progetto CCE, sia precedenti che oggetto della presente fornitura;
  - risoluzione di una richiesta di anomalia minore attraverso un intervento effettuato direttamente presso la sede dell'utente, ove possibile;
  - Pianificazione bi-settimanale degli interventi di presidio *on-site* nei punti di erogazione sulla base delle criticità emerse dal monitoraggio ed eventuali richieste e segnalazioni degli utenti;

  La modalità di erogazione potrebbe anche essere effettuata in remoto (in via residuale e ove lo svolgimeto da remoto cpmporta dei vantaggi immediati per l'utente finale).

:

Tutti i malfunzionamenti rilevat in fase di affiancamento o assistenza on-site dovranno essere tracciati nel sistema di *trouble ticketing*. Tutte le richieste migliorative e/o evolutive dovranno essere riportate al Committente per opportuna analisi e approvazione.

Per lo svolgimento delle attività, si richiede la disponibilità di personale, permanentemente allocato, secondo una ripartizione da concordare in fase di esecuzione del contratto, pari a 16 risorse in servizio 7/7 dalle 8:00 alle 16:00.

Per quanto attiene ai requisiti e modalità di erogazione del servizio, al *team* di lavoro e alle metriche di dimensionamento si rimanda a quanto presente nel CTS Lotti applicativi al capitolo 4 relativamente al servizio oggetto del presente paragrafo.

Supporto specialistico (SS)

Il servizio comprende attività di supporto in ambito ICT all'Amministrazione con la finalità di assicurare risposte altamente specialistiche per indirizzare le scelte tecnologiche e di prodotto, comprendere trend tecnologici e opportunità di ottimizzazione dell'infrastruttura.
Si intendono attività propedeutiche ovvero integrative ovvero di ausilio ai servizi sia applicativi ed in particolare ai servizi realizzativi al fine di rendere sinergici ed esaustivi tutti i componenti della fornitura.
Tra le attività rientrano a titolo esemplificativo e non esaustivo:

- supporto all'uso di nuovi prodotti applicativi;
- assessment del parco tecnologico esistente dal punto di vista delle tecnologie e delle architetture;
- benchmarking;
- supporto alla redazione di relazioni tecniche, redazione o validazione linee guida tecniche/metodologie interne; supporto all'analisi dei rischi, allo sviluppo di modelli e metodologie standard per la gestione degli stessi, alla definizione e controllo delle azioni correttive necessarie;
- supporto all'analisi comparata di scenari alternativi, realizzazione quadri di sintesi, prototipazione e simulazioni differenti rispetto alle attività che fanno parte delle fasi operative di analisi e progettazione dei servizi realizzativi di sw;
- Supporto per l'ottimizzazione delle applicazioni;
- supporto per eventi e presentazioni anche con sviluppo di prototipi di tipo "usa e getta" per esigenze dell'Amministrazione;
- esecuzione, realizzazione di sperimentazioni e prototipi che non comportino la produzione di codice o la scrittura di software.

Il fornitore dovrà, inoltre, disporre di competenze specialistiche verticali nei seguenti ambiti:

- trend tecnologici: competenze specifiche sui trend tecnologici emergenti di interesse per la PA, che possono rappresentare fattori di ottimizzazione dei processi e delle applicazioni in chiave di trasformazione digitale;
- specializzazione Cloud: competenze specialistiche in ambito Cloud, dagli aspetti architetturali alla sicurezza, alla performance, alla gestione di soluzioni SaaS.

Si richiede inoltre supporto all'utilizzo dell'ambiente Regionale per la realizzazione di analisi in ottica di Self BI

Per quanto attiene ai requisiti e modalità di erogazione del servizio, al team di lavoro e alle metriche di dimensionamento si rimanda a quanto presente nel CTS Lotti applicativi al capitolo 4 relativamente al servizio oggetto del presente paragrafo.

Servizi di conduzione tecnica (CT)

Nell'ambito del servizio di Conduzione tecnica rientrano i seguenti ambiti di intervento:

- Presa in carico e messa in esercizio delle architetture e infrastrutture (hardware e software);
- Supporto nella messa in esercizio delle applicazioni e presa in carico delle stesse;
- Conduzione e gestione dei sistemi fisici e virtuali, degli apparati di sicurezza, di connettività, dello storage, della continuità operativa (Backup, Disaster/Recovery) dell'Amministrazione.

Per quanto attiene ai requisiti e modalità di erogazione del servizio, al team di lavoro e alle metriche di dimensionamento si rimanda a quanto presente nel CTS Lotti applicativi al capitolo 4 relativamente al servizio oggetto del presente paragrafo.

Supporto Tecnologico (ST)

L'Amministrazione richiede servizi di supporto tecnologico relative ai seguenti ambiti di attività a titolo esemplificativo:

- supporto all'uso di nuovi prodotti;
- supporto alla realizzazione dei progetti di evoluzione infrastrutturale dell'Amministrazione;
- realizzazione di business case, studi, analisi di fattibilità, valutazione costi/benefici delle iniziative IT;
- analisi del Mercato ICT e predisposizione di materiale informativo per l'Amministrazione;
- *assessment* del parco tecnologico esistente dal punto di vista delle tecnologie e delle architetture;
- definizione di soluzioni IT per l'efficienza dei servizi informativi ed individuazione della soluzione maggiormente rispondente alle esigenze dell'Istituto, anche in ottica make or buy;
- supporto all'analisi dei rischi, allo sviluppo di modelli e metodologie standard per la gestione degli stessi, alla definizione e controllo delle azioni correttive necessarie;
- supporto per attività di change management complesse;
- supporto alla virtualizzazione di infrastrutture fisiche nell'ambito del CED dell'Amministrazione (migrazione Phisical-to-Virtual);

- supporto alla migrazione e gestione di infrastrutture di tipo Cloud. In particolare, le principali attività ricomprese sono di seguito elencate:
  - analisi costi/benefici e fattibilità
  - progettazione di *virtual data center*/ VM
  - configurazione di *virtual data center* / VM
  - supporto per la definizione e configurazione delle *policy* di *backup*/*restore*
  - supporto per la progettazione di Virtual Private Cloud e di Virtual Data Center

Servizi accessori

Servizi di Service Control Room per Monitoraggio tecnico/applicativo

Si richiedono servizi per l'attività di monitoraggio tecnico/applicativo, con soluzione rese disponibili dal Fornitore stesso, per il monitoraggio di tutti gli apparati affidati in Conduzione tecnica (*server*, *storage*, *database*, *middleware*, ecc…) e per le applicazioni, secondo quanto indicato dall'Amministrazione in fase di presa in carico dei servizi e nel corso di vigenza contrattuale.
Particolarmente rilevante è il monitoraggio delle componenti applicative preposte alla gestione dei flussi informativi che investono il Repository Clinico Aziendale, quali: flusso di conferimento dalla CCE al Repository, flusso di conferimento dai Dipartimentali aziendali al Repository e flusso di alimentazione del Fascicolo Sanitario Elettronico da parte del Repository.
Detti flussi, realizzati in cooperazione applicativa, sono asincroni rispetto ai processi interni dei Sistemi oggetto di integrazione (Repository, CCE e Dipartimentali) e dunque rappresentano una intrinseca criticità in termini di recupero e riconciliazione delle transazioni in errore.
Il Fornitore deve monitorare costantemente , in tempo reale, le componenti infrastrutturali e applicative innanzi citate a garanzia della immediata presa in carico delle anomalie che potrebbero causare la mancata circolazione di dati e documenti clinici tra i Dipartimentali, il Repository e il FSE.
Quanto realizzato deve consentire anche il monitoraggio delle attività di Backup delle Cartelle Clinici o dei processi che il Fornitore metterà in atto per garantire la continuità del servizio a seguito di malfunzionamenti della rete di trasmissione dati oppure della piattaforma applicativa.
Inoltre, il Fornitore deve definire le procedure di recupero specializzandole per singolo caso di errore gestito dal sistema ricevente (p.e. nel caso di alimentazione di FSE da parte del Repository, è necessario definire le procedure per ogni codice errore restituibile dal FSE); dette procedure devono essere automatiche e possono anche coinvolgere gli aspetti organizzativi del servizio di Monitoraggio tecnico/applicativo richiedendo, laddove necessario, l'interevento del personale adibito al servizio in parola.

6 Requisiti non funzionali

Nel presente Capitolo si descrivono le caratteristiche non funzionale che la soluzione CCE dovrà soddisfare.

Aderenza a standard

Dal punto di vista di *standard* dati riveste, come meglio descritto nel paragrafo successivo, una particolare rilevanza lo standard FHIR.
Per quanto riguarda gli *standard* funzionali, l'*Electronic Health Record System* dovrà essere il punto di riferimento per la definizione delle funzionalità che devono essere presenti nella Cartella Clinica Elettronica. L'insieme di tali funzionalità viene raggruppato in:

- Direct Care: funzioni che influiscono direttamente sull'erogazione del servizio di cura;
- Supportive: caratteristiche che impattano indirettamente nel servizio clinico, come le funzioni gestionali, e servono come input agli altri sistemi informativi dell'ospedale (amministrazione, controllo di gestione, ecc.);
- Information Infrastructure: funzionalità che non riguardano l'attività di cura, ma sono infrastrutturali (ad es. sicurezza e privacy del paziente, efficienza del servizio e interoperabilità fra diversi moduli o sistemi, ecc.).

In termini di standard semantici dovranno essere soddisfatti almeno gli standard SNOMED CT ed OMOP.
Per gli standard sintattici, oltre alle differenti componenti di HL7 che supportano la messaggistica tra applicazioni

sanitarie presenti in azienda, dovrà essere soddisfatto almeno lo standard DICOM (Digital Imaging and Communications in Medicine) per i criteri per la comunicazione, la visualizzazione, l'archiviazione e la stampa di informazioni ed immagini di tipo biomedico.

Pneudoanonimizzazione

Si privilegiano soluzioni che al fine della gestione e trattamento dei dati sensibili, della loro memorizzazione negli archivi, della loro registrazione nei file di audit e di log adottano o prevedono l'introduzione di tecniche di pseudonimizzazione e prevedono funzionalità a elevata sicurezza per l'anonimizzazione reversibile e/o la pseudonimizzazione dei dati, in modo da proteggere la confidenzialità delle informazioni relative ai pazienti, permettendo però (dati pseudonimizzati) la correlazione di dati riferiti allo stesso paziente ("record linkage"). Si restingono le operazioni di record linkage ai campi anagrafici pseudonimizzati.

Si privilegiano soluzioni che hanno o prevedono separazione del database dei dati anagrafici dei pazienti dal database impiegato invece per la gestione dei dati di attività della soluzione. La separazione anche fisica degli ambienti elaborativi e dei database utilizzati contribuisce a elevare la protezione dei dati sensibili gestiti.

Si precisa che le procedure che consentiranno di effettuare la pseudoanonimizzazione saranno definite nel corso del Contratto Esecutivo in base alle soluzioni disponibili (area applicativa SAP – Sistema di anonimizzazione e pseudoanonimizzazione).

Accessibilità e usabilità

Il sistema dovrà garantire:

- Rapidità di accesso alle funzioni chiave del sistema (ad es. presenza di menù generale con le aree applicative principali);
- Presenza in ogni schermata delle informazioni critiche sul paziente configurabili (ad es. anagrafica, avvisi su intolleranze/allergie, cadute accidentali, stati di iperpiressia, lesioni da decubito, contenzioni, ecc.);
- Supporto agile al work-flow clinico (per ambulatoriale ad es.: passaggio rapido tra le fasi di inquadramento, diagnosi, rilevazioni; per CCE di ricovero ad es.: link rapidi a scale di valutazione del dolore nell'area delle rilevazioni infermieristiche);
- La visualizzazione dell'intero percorso clinico del paziente in forma cronologica e sintetica, dando inoltre la possibilità di accedere al dettaglio di ciascun evento clinico occorso;
- Agli operatori di mettere in risalto le informazioni ritenute più rilevanti, quali: eventi critici occorsi, notevoli cambiamenti nelle condizioni del paziente, prossimi esami/accertamenti (tali informazioni dovranno essere organizzate in modo omogeneo e con una nomenclatura chiara e pertinente);
- La visualizzazione delle informazioni circoscritte all'ambito operativo dell'utente (reparto, ambulatorio, amministrazione, ecc.) e quindi di limitare i dati modificabili/inseribili a seconda dei diritti dell'operatore che si autentica al sistema, facilitando nel contempo la compilazione attraverso l'introduzione di frasi standardizzate nei campi di testo libero (il sistema dovrà dunque essere adattativo);
- Accesso mediante un unico insieme di credenziali definito dall'Amministrazione basato su identificazione tramite dispositivo (tramite smart-card operatore SISS, RFId, ecc.) o sistema di Single Sign-on aziendale e la trasparenza del cambio di contesto tra moduli o applicazioni differenti, senza quindi soluzione di discontinuità alcuna;
- Meccanismi volti a "sloggare" l'operatore nel caso in cui non effettui transazioni, di tipologie definite, per un tempo stabilito. Questi meccanismi dovranno essere configurabili per la definizione del tempo di inattività e per la definizione delle tipologie di transazioni che, se eseguite, azzerano il tempo di inattività;
- La gestione dettagliata e flessibile della profilazione degli utenti. Per ogni modulo o ambito di utilizzo della CCE dovrà essere possibile definire gli operatori abilitati a svolgere le diverse operazioni previste (ad es. creazione, modifica, visualizzazione, ecc.). I profili individuati dovranno poter essere applicabili a livello di operatori, gruppo di operatori, reparto, ecc.
- L'integrazione con dispositivi basati su tecnologie a codice a barre e RFId, come i braccialetti o badge, per l'identificazione dei pazienti;

- Una grafica semplice e con combinazioni di colori “comode” per la vista. Attraverso un’unica interfaccia, l’utente dovrà poter avere tutto il processo sotto controllo, in modo tale da reperire le informazioni in maniera più agevole e minimizzare l’apertura di ulteriori videate/popup durante la sessione di lavoro;
- Un’organizzazione dei singoli inserimenti in più campi, suddivisi in base alla sezione del documento, strutturati ad es. tramite checkbox, menu a tendina, ecc. per facilitare la manipolazione ed il riuso successivo delle informazioni;
- Interfaccia di tipo responsive per la fruizione efficace ed efficiente della soluzione anche in mobilità tramite tablet;
- Funzionalità di dettatura vocale con dizionario medico;
- Il supporto delle funzionalità di appunti del sistema operativo (“copia e incolla”);
- La firma digitale multidocumento;
- Ai fini della gestione del versioning dei documenti, la visualizzazione delle differenze nel testo tra la versione oggetto di firma e la sua eventuale versione precedente;
- Gestione di frasi standard per utente e/o specialità come supporto alla compilazione;
- L’accesso tramite standard W3C.

Efficienza ed Efficacia

La ridondanza del dato dovrà essere minimizzata al fine di ottenere maggior correttezza e puntuale aggiornamento.
Il requisito fondamentale di modularità della CCE dovrà permettere di scindere le funzionalità specifiche dei differenti ambiti operativi (specialità mediche, unità organizzative o gruppi clinici) da quelle comuni e quindi configurare i dati da presentare a seconda dell’ambito di afferenza dell’utente.
Dovrà essere evitata, tramite specifici controlli sui campi, l’eventualità che gli operatori omettano dati fondamentali per il percorso di cura o li scrivano in modo incompleto o sintatticamente scorretto.
È necessario che l’applicativo di CCE sia in grado di fornire una reportistica su temi quali: indicatori chiave di processo, gestione del rischio clinico, inconsistenze nei dati inseriti, statistiche a vari livelli sui casi clinici trattati (patologie manifestate, procedure/azioni terapeutiche attuate a livello medico ed infermieristico, prescrizioni e somministrazioni adottate, utilizzo di dispositivi, ecc.), statistiche di utilizzo dell’applicativo, e così via.
L’applicativo CCE dovrà prevedere sistemi di alert clinici significativi, automatici, oltre che di proposta di compilazione automatica di campi sulla base di altri elementi. Riguardo agli alert clinici significativi, questi dovrebbero avere le seguenti caratteristiche:

- Essere coerenti rispetto alla fase del percorso di cura;
- Essere il più possibile strutturati nei contenuti, limitando i campi testo di tipo aperto;
- Esprimere un’informazione essenziale che impatti sul rischio di vita della persona assistita (ad es. allergie);
- Essere in numero limitato per evitare l’eccesso delle informazioni.

È opportuno distinguere gli alert clinici significativi, scelti da parte dell’Amministrazione dopo condivisione interna con i professionisti, e gli “avvisi” che possono essere anche molto più numerosi, contestualizzati in specifici percorsi o per disciplina, pur sempre di univoca interpretazione e definizione a livello aziendale.
A tal proposito, la CCE dovrà prevedere dei meccanismi che consentano, nel caso in cui vengano apportate modifiche ad informazioni contenute nella CCE stessa, di notificare all’utente che esiste una versione nuova e aggiornata di tale informazione.
La CCE dovrà, inoltre, garantire un livello minimo per quel che riguarda le prestazioni ed in particolar modo i tempi di risposta delle diverse schede che la compongono, anche a fronte di richieste multiple provenienti dai diversi utenti.
Un’adeguata registrazione delle informazioni può rendere più efficiente l’erogazione delle prestazioni aumentando il tempo che il professionista può dedicare al paziente.
Un’adeguata registrazione delle informazioni può aumentare la soddisfazione del paziente facilitando attività integrate con l’erogazione della prestazione (prescrizioni di farmaci e accertamenti, certificazioni).
Al fine di evitare possibili inserimenti erronei, l’applicativo di CCE non dovrà consentire allo stesso operatore di aprire contemporaneamente due fascicoli elettronici di ricovero appartenenti a differenti persone assistite.
Infine, a supporto di tale requisito, si richiede che l’applicativo di CCE sia anche di ausilio nella fase di supporto decisionale all’utente, con specifiche funzionalità.

Disponibilità

La completa disponibilità dei dati clinici dovrà essere garantita sempre e dovunque, anche a fronte di un malfunzionamento del sistema, dell'infrastruttura di comunicazione o di altri sistemi applicativi integrati dell'Amministrazione

Dovranno, inoltre, essere adottati meccanismi che consentano l'attribuzione di identificativi provvisori da parte della CCE nei casi in cui il sistema di competenza sia indisponibile (ad es. codice nosologico in caso di ADT indisponibile) da riconciliare una volta ripristinato il sistema.

La CCE dovrà essere coerente con contesto organizzativo dell'Amministrazione e le relative procedure di emergenza e *business continuity*.

Estendibilità e scalabilità

Dovrà essere possibile estendere di volta in volta la CCE con le funzionalità dei vari reparti specialistici o organismi dell'Amministrazione interessati a tali dati. I requisiti di scalabilità dovranno essere rispettati per tutte le componenti rientranti nel progetto CCE, compreso il Repository clinico Aziendale e la sua capacità di alimentare il FSE, attraverso un giusto dimensionamento delle infrastrutture di calcolo, di rete, di archiviazione dati.
Il sistema dovrà possedere:

- Scalabilità di carico, ovvero capacità di aumentare le prestazioni del sistema in funzione della potenza di calcolo complessiva dedicata alla sua esecuzione. Tale scalabilità è necessaria per far fronte al carico computazionale generato dall'ingente e sempre crescente numero di utenti utilizzatori del sistema.;
- Scalabilità geografica, intesa come capacità del sistema di mantenere inalterata la sua usabilità e utilità indipendentemente dalla distanza fisica dei suoi utenti o delle sue risorse. Nel sistema, dunque, dovranno essere integrate sedi periferiche dell'Amministrazione;
- Scalabilità clinica, ovvero necessità di coprire specifiche esigenze del processo di cura in ambiti operativi ad alta specializzazione (come ad es. i reparti di Rianimazione e Terapia Intensiva). Essa dovrà essere garantita sia dalla flessibilità della CCE aziendale, sia dalla presenza di moduli applicativi verticali integrati con il sistema aziendale stesso. Queste valutazioni dovranno essere condotte di concerto con la funzione aziendale preposta al governo dell'architettura del Sistema Informativo Aziendale, nell'ottica di salvaguardare la coerenza del Sistema Informativo Aziendale;
- Scalabilità amministrativa, ovvero mantenere inalterata la sua gestibilità indipendentemente da quante organizzazioni lo utilizzano.

Tracciabilità ed esibizione

L'applicativo di CCE dovrà continuare a garantire la tracciabilità totale delle operazioni, ossia dovrà tener traccia, per ciascuna operazione di accesso, visualizzazione, inserimento, modifica o importazione, delle informazioni relative a data, ora e autore della operazione, dandone evidenza a livello di interfaccia ove richiesto.
Dovrà sempre essere attivo il meccanismo di salva in bozza, antecedente al perfezionamento di un documento e alla sua pubblicazione, oltre che di tracciabilità della data e dell'ora di registrazione dell'informazione. Si precisa che la bozza dovrà essere accessibile unicamente al suo redattore e sottratta alla pubblicazione, operazione quest'ultima da riservarsi unicamente ai documenti perfezionati.
La CCE dovrà garantire inoltre che, fatte salve le bozze, le informazioni registrate siano rese non modificabili e storicizzate.
La CCE dovrà altresì consentire la possibilità di attivazione una validazione/approvazione esplicita, da parte dei soggetti autorizzati, dei documenti/dati ricevuti automaticamente da fonti esterne (ad es. referti, dati di laboratorio, di monitoraggio, ecc.). Qualora attivata, eventuali documenti/dati non ancora validati e quindi non facenti ancora parte della CCE, dovranno comunque essere fruibili dando evidenza del loro stato di validazione.
L'estrazione di copie analogiche di originali informatici, seppur possibile, dovrà avvenire con indicazione chiara della fonte e nel rispetto di eventuale regolamentazione aziendale.
Un aspetto particolare dell'estrazione di dati si presenta quando sia richiesta l'esecuzione di una prestazione sanitaria in struttura diversa da quella di ricovero dell'assistito. I sanitari della struttura erogante dovranno poter

conoscere le informazioni raccolte nella CCE formata fino a quel momento.

Consegna e versionamento del Software

Il software sviluppato e relativa documentazione deve essere consegnato tramite l'utilizzo del sistema di gestione del versionamento che sarà individuato e reso disponibile dal Committente, le cui modalità e credenziali d'accesso saranno comunicate alla Ditta Aggiudicataria dopo l'aggiudicazione della gara.
Il Committente si riserva di chiedere la contestuale consegna di una copia del software anche su supporto magnetico/ottico.
La frequenza di riversamento, da parte della Ditta Aggiudicataria nel sistema di gestione del versionamento, sarà definita dal Committente in fase esecutiva, anche in funzione degli interventi di manutenzione che saranno realizzati.
In caso di indisponibilità del servizio di Gestione del versionamento verranno concordate con il Committente diverse modalità di consegna.
Vi è comunque l'obbligo della Ditta Aggiudicataria di accompagnare la consegna con la *Release Notes* completa di tutte le informazioni necessarie per la gestione del versionamento.
Tutti i prodotti ed i documenti consegnati dovranno essere esenti da virus. Il Committente si riserva di verificare l'assenza di virus secondo le modalità e gli strumenti che riterrà più opportuni.
Per la documentazione del codice sarà utilizzato Javadoc ove applicabile o equivalente strumento di documentazione del codice sorgente.

7 REQUISITI SICUREZZA

Di seguito sono riportati i requisiti di sicurezza che la Cartella Clinica Elettronica deve garantire. I requisiti vengono mappati su un modello formato da diversi Domini di pertinenza, ognuno dei quali identifica uno specifico ambito di sicurezza, che sarà descritto nel dettaglio nella sezione successiva:

- Infrastructure Domain;
- Identity Domain;
- Data Domain;
- Application Domain;
- Monitoring Domain;
- Response Domain.

L'attività di governance della Regione Puglia, in continua evoluzione, potrebbe originare la disponibilità di infrastrutture e servizi di sicurezza centralizzati gestiti dallo CSIRT Puglia, che possono aiutare sia la Regione Puglia che il fornitore nella predisposizione degli stessi servizi di sicurezza. Pertanto, il fornitore è tenuto a verificare tali disponibilità consultando il portale CSIRT Puglia alla URL https://csirt.puglia.it.

Lo CSIRT Puglia eroga servizi di sicurezza, di monitoraggio della resilienza dei sistemi informativi e di supporto alla fase di gestione incidenti e di analisi dei rischi.

Preliminarmente al collaudo e/o alla messa in esercizio, il Fornitore dovrà fornire evidenze oggettive, che confermino che quanto riportato nel Piano della Sicurezza (di seguito PdS) sia stato effettivamente implementato e/o predisposto affinché si possano raggiungere gli obiettivi di sicurezza fissati dallo stesso Piano. Al fine di di garantire, monitorare e controllare la sicurezza dei sistemi informativi a supporto del sistema della Cartella Clinica Elettronica, è necessario che il Fornitore si attenga alle indicazioni riportate nel PdS. Il PdS rappresenta, infatti, l'insieme delle indicazioni di natura tecnologica, organizzativa e procedurale che ogni organizzazione è obbligata ad adottare per assicurare un adeguato livello di sicurezza informatica. Nell'attuazione di tale approccio, il Fornitore deve mirare al conseguimento della massima sicurezza dei servizi.

A tal fine, il Sistema ed i servizi devono essere sottoposti a periodiche scansioni per identificare eventuali vulnerabilità all'interno delle applicazioni in fase di esecuzione e l'analisi dell'esposizione al rischio di attacchi informatici ai sistemi informativi mediante l'utilizzo di tecniche di analisi statica e dinamica.

Indipendentemente dalle verifiche richieste ed effettuate dal Fornitore, la Stazione Appaltante si riserva di effettuare, tramite il CSIRT Regionale, controlli periodici tramite l'esecuzione di Vulnerability Assessment (VA), Web Application Scanning (WAS) e Penetration Test (PT), necessari per certificare la sicurezza dei sistemi oggetto dell'appalto. L'attività di Vulnerability Assessment è condotta per identificare eventuali vulnerabilità informatiche presenti nel sistema informativo. L'attività di Penetration Test è condotta per simulare attacchi informatici mirati ai sistemi, al fine di produrre un dettagliato report su ciò che è stato identificato e sviluppare piani di rientro. Tale attività sarà concordata con il Fornitore.

Il Fornitore sarà obbligato ad attuare tutte le contromisure e i piani di rientro necessari a correggere le vulnerabilità riscontrate dai controlli eseguiti. La Stazione Appaltante si riserva di rieseguire i controlli a termine della bonifica delle criticità evidenziate.

Il mancato superamento delle verifiche del software oggetto di nuovo rilascio costituisce non conformità della fornitura, mentre analogo esito in fase di esercizio rende necessario e improrogabile un intervento di manutenzione correttiva, al fine di rendere il sistema nuovamente sicuro.

Il Fornitore, con l'accettazione del presente capitolato, per l'esecuzione dei security assessment si rende disponibile a supportare le verifiche, consapevole del rischio residuo, ancorché minimo, che gli stessi possano interferire con l'erogazione del servizio. La Stazione Appaltante si impegna comunque a garantire che le operazioni, eseguite direttamente e/o per il tramite di soggetti terzi, siano confinate nei limiti esclusivi della finalità di verifica della sicurezza del sistema informativo ed informatico interessato ed a non cagionare alcuna alterazione o manomissione dei dati in esso contenuti e del livello di servizio.

Analogamente, costituisce valida motivazione per un intervento di manutenzione correttiva, la segnalazione di criticità di sicurezza da parte di autorità nazionali di controllo per la Cybersecurity (CERT/CSIRT Nazionale e/o Regionale, CNAIPIC, ecc.).

Inoltre, nell'ambito delle attività di monitoraggio continuo della Cybersecurity, il Fornitore ha l'obbligo di segnalare gli incidenti di sicurezza al CSIRT Puglia secondo modalità e procedure che saranno fornite nella fase esecutiva del contratto.

Relativamente ai requisiti di sicurezza, si precisa che il fornitore dovrà implementare quanto prescritto con soluzioni tecnologiche adeguate.

Raccolta dei requisiti

Il soddisfacimento dei requisiti di seguito riportati è da considerarsi mandatorio.

Infrastructure Domain

L'Infrastructure Domain si concentra sull'individuazione dei requisiti che è necessario implementare al fine di ridurre la potenziale superficie d'attacco interna, per evitare la presenza di misconfiguration o potenziali vulnerabilità. In particolare, il presente dominio individua i requisiti necessari ad una corretta hardenizzazione dell'ambiente e delle Golden Images utilizzate, individuando le modalità di segmentazione della rete, delle relative regole di gestione dei flussi di rete e delle modalità di mantenimento della documentazione tecnica.
Di seguito l'elenco dei requisiti identificati per questo dominio:

ID	Dominio	Argomento	Requisito	Tipologia
RS1	**Infrastructure Domain**	Accessi remoti	Al fine di garantire la protezione degli accessi remoti al Servizio, questi dovranno avvenire secondo modalità sicure, che implementano protocolli di	Configuration

ID	Dominio	Argomento	Requisito	Tipologia
			crittografia per garantire la riservatezza e l'integrità dei dati trasmessi attraverso la rete	
RS2	**Infrastructure Domain**	PAM	Gli accessi amministrativi all'infrastruttura ospitata sul Datacenter devono essere gestiti e monitorati mediante una soluzione PAM. La soluzione PAM da utilizzare è quella resa disponibile dalla Regione Puglia attraverso l'azione dello CSIRT Puglia. Il fornitore potrà definire e monitorare i propri Amministratori di Sistema (AdS), con lo CSIRT Puglia che, in segregation of duties, potrà garantire la supervisione delle attività compiute dagli AdS.	Technology/ Technical control
RS3	**Infrastructure Domain**	Remote access	Al fine di mettere in sicurezza gli accessi remoti all'infrastruttura ospitata sul Datacenter, il servizio deve rispettare i seguenti requisiti: • Tutti i punti di accesso che consentono l'accesso esterno all' infrastruttura ospitata sul Datacenter devono essere documentati e monitorati. • È necessario utilizzare una soluzione di mercato VPN per proteggere gli accessi all'infrastruttura ospitata sul Datacenter provenienti da Internet. • L'accesso remoto deve supportare l'implementazione dei principi di Zero Trust (ad esempio, segmentazione e accesso basati su identità/conformità) • Gli accessi dovranno prevedere forme di autenticazione a due fattori	Technology/ Technical control
RS4	**Infrastructure Domain**	Endpoint Protection	Al fine di assicurare una efficace cornice di sicurezza, si richiede sia installata e gestita una soluzione di ***endpoint protection***: • che consenta di ricostruire l'eventuale *killchain* posta in essere dall'agente di minaccia • che offra un motore di analisi comportamentale (*behavioral analysis*) al fine di identificare divergenze rispetto al normale comportamento posto in essere dagli utenti • che garantisca aggiornamento tempestivo delle firme identificanti archiviazione ed esecuzione codici malevoli. Inoltre, si richiede che eventuali compromissioni vengano anche notificate allo CSIRT Puglia, previa registrazione al portale https://csirt.puglia.it	Technology/ Technical control
RS5	**Infrastructure Domain**	Cloud Workload Protection	Deve essere adottato un sistema di *Cloud Workload Protection Platform* per la protezione dei container presenti all'interno dall'ambiente	Technology/ Technical control

ID	Dominio	Argomento	Requisito	Tipologia
RS6	**Infrastructure Domain**	Documentation	Il Servizio deve implementare un adeguato processo di documentazione: • gli owner e le loro responsabilità devono essere documentati e comunicati; • deve essere identificato e mantenuto un sistema di *Knowledge Base* o in un repository centrale a cui è assegnato un owner; • deve essere mantenuta una documentazione tecnica afferente all'infrastruttura che includa: diagramma infrastrutturale, flussi di rete, flussi dei dati, range IP interni e range IP pubblici, porte utilizzate dai servizi esposti.	Documentation /Procedure
RS7	**Infrastructure Domain**	Firewall	Il Servizio deve essere protetto da un sistema di **Firewalling** con cui devono essere implementate adeguate policy e regole: • un NGFW (Next Gen Firewall) deve essere implementato in qualsiasi punto in cui i dati vengono trasmessi tra infrastruttura ospitata sul Datacenter e le reti pubbliche; • ogni segmento di rete interno deve essere soggetto alla protezione e segmentazione di un NGFW; • il NGFW utilizzato non deve consentire regole *any-to-any* in entrata/uscita su tutte le porte; • il NGFW deve applicare misure di Intrusion Prevention o Detection per tutti i flussi dati inter-zona; • sul NGFW vanno configurate le regole FW utili a garantire solo il traffico necessario al funzionamento della soluzione.	Technology/ Technical control
RS8	**Infrastructure Domain**	Golden Images	I seguenti requisiti afferiscono ad una adeguata gestione e protezione delle ***Golden Images*** che il Servizio deve implementare: • definizione di una gold standard image per il deploy di ogni nuova istanza di VM; • la golden images definita deve essere hardenizzata secondo gli standard e le best practices (es. CIS Benchmark level 1, vendorprovided standards, etc.); • le golden images devono sempre essere utilizzate quando si deployano nuove istanze di macchine virtuali.	Configuration
RS9	**Infrastructure Domain**	Hardening	Tutte gli asset devono essere soggetti a processo di hardening secondo le seguenti linee guida: • le Cloud Subscriptions e i container devono essere hardenizzati secondo gli standard e le best practices (es. CIS Benchmark level 1, vendor-provided standards, etc.); • tutte le risorse non cloud (ad esempio, macchine	Configuration

ID	Dominio	Argomento	Requisito	Tipologia
			virtuali) devono essere hardenizzate in base a standard e best practice (es. CIS Benchmark livello 1, standard forniti dal fornitore, etc.) prima della distribuzione alla produzione. In aggiunta, sono in capo al fornitore le seguenti attività relative all'hardening dei sistemi: • definire gli indicatori (processi attivi, applicazioni installate, utenti gestiti, password policy, etc.) da usare per la definizione del livello di sicurezza del sistema; • effettuare statistiche per valutare l'andamento nel tempo di tali indicatori; • reperire, creare o personalizzare gli opportuni strumenti atti a monitorare la configurazione di ogni sistema	
			• individuare e segnalare eventuali criticità nella configurazione dei sistemi maggiormente critici; • intraprendere, a fronte di criticità di sicurezza emerse dalla fase di monitoraggio e analisi, gli opportuni interventi correttivi che riportino il sistema al livello di sicurezza desiderato.	
RS10	**Infrastructure Domain**	Network Architecture	Al fine di garantire un design e un'implementazione che consideri gli aspetti di sicurezza fin dalle prima fasi del progetto, si richiede che l'architettura di network del servizio, integri i seguenti principi: • deve essere garantita un'opportuna segregazione delle reti al fine di garantire la riduzione della superficie d'attacco e un maggiore controllo sui flussi dei dati; • devono essere implementate misure (es. ridondanza, alta affidabilità, etc.) per contrastare i *single point of failure*; • le interfacce di diagnostica e configurazione devono essere identificate, documentate e protette da accessi non autorizzati o disattivate completamente; • è necessario utilizzare protocolli sicuri durante le comunicazioni tra i livelli infrastrutturali e applicativi (es. SFTP per la condivisione di file);	Configuration
RS11	**Infrastructure Domain**	Security Solutions Management	Il fornitore deve assicurare la qualità di tutte le attività per la gestione del ciclo di vita delle policy/regole applicate agli apparati di sicurezza (firewall, security web gateway, sistemi anti DDoS, …) e un attento controllo di ogni cambiamento. Viene, pertanto, richiesto al fornitore di gestire tutte le fasi di implementazione delle regole di	Documentation /Procedure

ID	Dominio	Argomento	Requisito	Tipologia
			sicurezza. Nello specifico si identificano le seguenti fasi: 1) ricezione delle richieste di variazione; 2) registrazione delle richieste e classificazione; 3) analisi di impatto della richiesta; 4) valutazione del rischio nell'implementare	
RS12	**Infrastructure Domain**	WAF Protection	Le applicazioni e i sistemi esposti verso Internet (es. gateway API, etc.) devono essere protetti da un presidio di sicurezza a livello applicativo (es. WAF).	Technology/ Technical control
RS13	**Infrastructure Domain**	DoS Protection	Al fine di una efficace protezione da attacchi di tipo *denial of service*, il Servizio deve implementare un meccanismo efficace contro DoS che deve prevedere: • protezione contro attacchi di tipo *volume-based*; • sistema automatizzato di *prevention e remediation anti-DoS*.	Technology/ Technical control
RS14	**Infrastructure Domain**	IDPS	Un presidio di Intrusion Prevention o Detection deve essere implementato per tutte le applicazioni esposte verso Internet per prevenire e rispondere agli attacchi basati su firme e rilevamento di anomalie.	Technology/ Technical control

Tabella 5: Tabella dei Requisiti di Sicurezza (RS) relativi all'Infrastructure domain

Identity domain

L'identity domain permette di gestire centralmente utenti e gruppi che possono accedere alle risorse a seconda dei loro ruoli e dei loro privilegi. In particolare, il presente dominio tratta i diritti e i ruoli che vengono concessi agli utenti e le corrette modalità di autenticazione.
E' disponibile il sistema di Identity and Access Management (IAM) regionale che viene utilizzato per fornire l'accesso a norma CAD (SPID/CIE/CNS/EIDAS) a tutti i sistemi federati; oltre a questi è possibile anche integrare in IAM i repository di utenti esterni in formato ldap, active directory o su DB relazionale, che possono essere integrati per garantire la continuità di uso delle credenziali normalmente utilizzate dagli utenti di un determinato sistema applicativo o dominio.
IAM gestisce esclusivamente la fase di autenticazione: tutti gli aspetti autorizzativi e di gestione degli utenti vengono demandati al servizio applicativo federato.
La piattaforma contiene tutte le funzionalità di gestione degli utenti, rivolte sia agli utenti contenuti nel repository primario (interni) o in quelli secondari (ldap esterni); tuttavia, gli ldap esterni sono solitamente di proprietà di enti esterni (tipicamente le ASL), per cui l'integrazione di questi ldap viene effettuata in modalità sola lettura e viene utilizzata esclusivamente per l'autenticazione.
Il fornitore, utilizzando le funzionalità già disponibili di IAM (specifiche disponibili al link https://www.rupar.puglia.it/iam), dovrà realizzare le funzionalità di Identity Domain secondo i requisiti riportati nella tabella sottostante.
Il Fornitore deve progettare, descrivere e realizzare una soluzione applicativa che consente l'accesso alla piattaforma di CCE anche in assenza della connesione del sistema IAM regionale al singolo LDAP aziendale.

ID	Dominio	Argomento	Requisito	Tipologia

ID	Dominio	Argomento	Requisito	Tipologia
RS15	**Identity Domain**	Access Rights	Per una corretta gestione della sicurezza relativa al controllo degli accessi e alla gestione degli utenti, il servizio deve sottostare ai seguenti principi: • Least Privilege: all'utente devono essere assegnati soltanto i permessi minimi necessari all'esecuzione delle attività assegnate. • Segregation of Duties: l'accesso, i ruoli e i permessi che comportano un potenziale conflitto di interessi per un singolo utente non devono essere assegnati contemporaneamente	Configurazione
RS16	**Identity Domain**	IAM	Il servizio deve utilizzare un sistema di Identity and Access Management per la gestione del ciclo di vita degli utenti.	Controllo tecnico/Tecnologia
RS17	**Identity Domain**	Authentication	Il servizio deve consentire l'integrazione con piattaforme esterne di gestione dell'identità attraverso l'utilizzo di protocolli standard quali: LDAP, SAML 2.0 e OAuth 2.0.	Controllo tecnico/Tecnologia
RS18	**Identity Domain**	Authentication	Il servizio deve consentire l'integrazione con il SISS. L'accesso alla CCE da parte di utenti delle Strutture Sanitariee avverrà tramite autenticazione con il SISS e sue evoluzioni (es. SISS3) sfruttando meccanismi di MFA e SSO.	Controllo tecnico/Tecnologia

ID	Dominio	Argomento	Requisito	Tipologia
RS19	**Identity Domain**	Role Based Access Control	Il servizio deve prevedere un modello autorizzativo di tipo RBAC per garantire una gestione efficace e granulare degli accessi degli utenti alle funzionalità e alle informazioni del sistema. Tale modello deve garantire le seguenti funzionalità: • Definizione dei ruoli: il servizio deve consentire di definire ruoli diversi in funzione delle diverse esigenze operative (es. amministratore di sistema, utente standard, tecnico di supporto, etc.). • Controllo dei privilegi: il servizio deve consentire, per ciascun ruolo, la configurazione dei privilegi di accesso alle risorse ed alle funzionalità ad esso associati. • Assegnazione dei ruoli: gli utenti devono essere assegnati a ruoli appropriati alle loro responsabilità e in base alle specifiche necessità di accesso a informazioni e funzionalità. • Gestione dei ruoli: il servizio deve consentire di suddividere gli utenti in gruppi, con esigenze operative omogenee, e di assegnare i diversi ruoli a tali gruppi anziché prevedere una assegnazione specifica per singolo utente, semplificando in tal modo la gestione e il controllo dei privilegi assegnati nel rispetto del principio di Least Privilege. • Accesso basato su regole: il servizio deve consentire di definire regole di accesso che determinino quali utenti o ruoli possono accedere a determinate risorse o eseguire determinate azioni. • Gestione centralizzata: il servizio deve consentire una gestione centralizzata per la gestione dei ruoli, delle regole e degli utenti, al fine di semplificare l'amministrazione e garantire la coerenza nell'applicazione delle politiche di accesso.	Configurazione
RS20	**Identity Domain**	MFA	Il servizio deve supportare l'integrazione con soluzioni esterne di Multi-Factor Authentication (MFA)	Controllo tecnico/Tecnologia
RS21	**Identity Domain**	Privileged Accesses	Il servizio deve supportare l'integrazione con soluzioni esterne per la gestione delle identità privilegiate (es. Privileged Access Management – PAM)	Controllo tecnico/Tecnologia

ID	Dominio	Argomento	Requisito	Tipologia
RS22	**Identity Domain**	Default vendor accounts and default vendor passwords	Gli account di default di eventuali componenti utilizzati all'interno del servizio devono essere rimossi o disabilitati. Se un account di default non può essere rimosso o disattivato, la password di default associata deve essere modificata al momento dell'installazione del componente.	Configurazione
RS23	**Identity Domain**	Account passwords	Per poter garantire una corretta protezione della password e del meccanismo di autenticazione, le credenziali di accesso non devono mai essere conservate come dati in chiaro. I requisiti di robustezza e gestione delle password devono essere conformi a quanto definito nelle linee guida Agid declinate nel documento "*Misure minime di sicurezza ICT per le pubbliche amministrazioni*". In ogni caso, il Fornitore dovrà garantire l'implementazione di misure di sicurezza che garantiscano un elevato livello di protezione della gestione delle password secondo quanto suggerito dalle Best Practices e dagli Standard Settore.	Configuration
RS24	**Identity Domain**	IAM Secure Configuration	Al fine di garantire un adeguato livello di protezione della soluzione utilizzata per la gestione delle Identity, dovranno essere implementati i seguenti requisiti: • minimizzazione del numero di utenze e gruppi privilegiati • implementazione di meccanismi di password enforcing per tutte le utenze privilegiate • Implementazione di meccanismi di sicurezza e monitoring dei Service Account • qualora previste, disattivazione delle utenze locali di administrator • abilitazione di Audit Policy afferenti alle utenze privilegiate • raccolta log e monitoring delle utenze privilegiate e service account • revisione periodica di tutte le utenze al fine di individuare utenze inattive	Configuration
RS25	**Identity Domain**	Local accounts	Eventuali credenziali locali o di root per l'accesso a sistemi e risorse nel cloud devono essere	Configuration

ID	Dominio	Argomento	Requisito	Tipologia
			cancellate/disabilitate, ove possibile, preferendo l'accesso tramite utenti gestiti dallo IAM.	
RS26	**Identity Domain**	Timeouts for SSO enabled applications	Per gli account non privilegiati, l'intera durata del token/sessione non deve superare i 5 giorni, compresi i meccanismi di estensione della validità del token ("refresh token"), mentre per gli account privilegiati, l'intera validità del token/sessione non deve superare un massimo di 12 di estensione della validità del token ore, compresi i meccanismi	Configurazione

Tabella 6: Tabella dei Requisiti di Sicurezza (RS) relativi all'Identity domain

Data domain

Il data domain si concentra sulla classificazione automatica e continua, sull'archiviazione e sul trasferimento dei dati in modo sicuro. In particolare, il presente dominio tratta la sicurezza del dato indicando i requisiti crittografici e i processi da implementare per una corretta gestione della sicurezza delle informazioni e dei dati personali.
Di seguito l'elenco dei requisiti identificati per questo dominio:

ID	Dominio	Argomento	Requisito	Tipologia
RS27	**Data Domain**	Encryption	Al fine di garantire adeguata protezione dei dati in transito (in transit) il servizio deve garantire: • La cifratura delle comunicazioni in ingresso ed in uscita dallo stesso attraverso protocolli crittografici standard (es. TLS 1.2 e superiori). • La cifratura delle comunicazioni attraverso le differenti componenti applicative dello stesso attraverso protocolli crittografici standard (es. TLS 1.2 e superiori).	Controllo tecnico/Tecnologia
RS28	**Data Domain**	Encryption	Al fine di garantire adeguata protezione dei dati memorizzati (at rest) il servizio deve garantire: • funzionalità di anonimizzazione e pseudonimizzazione dei dati, ove richiesto, durante il trattamento degli stessi; • funzionalità di encryption dei dati memorizzati nei database e sugli apparati di archiviazione collegati allo stesso; • che la soluzione di crittografia selezionata implementi misure di sicurezza contro gli attacchi di brute-force offline (ad esempio utilizzando un Trusted Platform Module); • Nel caso tali misure di sicurezza non fossero applicabili, la password utilizzata per la	Controllo tecnico/Tecnologia

ID	Dominio	Argomento	Requisito	Tipologia
			crittografia deve essere lunga almeno 30 caratteri e deve soddisfare i requisiti di complessità da best practice.	
RS29	**Data Domain**	Test Data	I dati utilizzati a fini di test devono: • essere generati, anonimizzati ed etichettati come dati di test; • essere utilizzati solamente in ambienti di test/sviluppo. Nel caso i dati di test siano ricavati partendo da dati reali deve essere garantito che non si possano ricavare da essi informazioni riconducibili al dato di partenza. Nel caso in cui dati di produzione vengano utilizzati in ambiente di test o di sviluppo, questi dati devono essere anonimizzati.	Configurazione

Tabella 7: Tabella dei Requisiti di Sicurezza (RS) relativi al Data domain

Application domain

L'application domain si concentra sul seguire automaticamente e continuamente un Secure Software Development Life Cycle. In particolare, il presente dominio tratta la sicurezza applicativa quale potenziale perimetro in cui è necessario prevenire la presenza di potenziali vettori d'attacco. I requisiti indicati afferiscono alle corrette modalità di gestione della sicurezza delle API e all'effettuazione periodica di security assessment al fine di individuare la presenza di potenziali nuove vulnerabilità applicative.
Di seguito l'elenco dei requisiti identificati per questo dominio:

ID	Dominio	Argomento	Requisito	Tipologia
RS30	**Application Domain**	Least Functionality principle	Il servizio deve esporre soltanto le funzionalità e i servizi necessari al corretto funzionamento e allo svolgimento delle attività prestabilite, rimuovendo o disabilitando tutti i componenti e/o le funzionalità non necessarie e/o potenzialmente non sicure, al fine di ridurre al minimo la superficie di esposizione esterna.	Configurazione
RS31	**Application Domain**	API Security management	Il servizio dovrà garantire e supportare: • la crittografia TLS (1.2 o superiore) per le API al fine di assicurare la riservatezza dei dati; • l'attivazione delle funzionalità di API e IP Whitelisting per ridurre il perimetro di esposizione; • il rispetto delle linee guida AGID in	Controllo tecnico/Tecnologia

ID	Dominio	Argomento	Requisito	Tipologia
			materia di API security.	
RS32	**Application Domain**	Security Assessment	Devono essere pianificate ed effettuate attività di vulnerability assessment ricorrenti, e almeno a cadenza annuale o a fronte di ogni rilascio pianificato, al fine di prevenire ed individuare potenziali vettori d'attacco: • un vulnerability assessment infrastrutturale su tutti i componenti dell'architettura deve essere eseguito prima del deployment in produzione; • un vulnerability assessment applicativo; • un vulnerability assessment sulle API utilizzate. Inoltre, le attività di scanning devono essere effettuate scongiurando il degrado delle prestazioni delle reti o altri eventi che possano provocare instabilità. Gli scanner devono essere sempre aggiornati rispetto alle ultime firme di vulnerabilità.	Documentazione/Procedure
RS33	**Application Domain**	Security Test	Devono essere pianificate ed effettuate attività di security testing ricorrenti, e almeno a cadenza annuale o a fronte di ogni rilascio pianificato, al fine di prevenire ed individuare potenziali vettori d'attacco: • Security Testing infrastrutturale interno (es. PT infrastrutturale, etc.); • Security Testing applicativo interno ed esterno (es. WAPT, etc.); • Security Testing sul codice (es. SAST, DAST, etc.) al fine di identificare potenziali bug, errori o debolezze all'interno del codice potenzialmente sfruttabili; • API Security Testing. Prima dell'effettuazione di una attività di security testing, deve essere prodotto un documento relativo alle Regole di Ingaggio in cui saranno definiti: • il blocco di rete e/o gli URL che saranno oggetto delle attività di testing; • i servizi e/o i sistemi oggetto delle attività di testing; • le fasce orarie in cui verranno effettuati i test. A valle dell'attività di testing dovrà essere prodotto un Report in cui sarà presente una parte di Executive Summary e una con il Dettaglio Tecnico, nonché un suggerimento delle misure di fixing da	

ID	Dominio	Argomento	Requisito	Tipologia
			apportare.	
RS34	**Application Domain**	SDLC	Le attività di sviluppo del codice devono seguire un processo di Software Development Lifecycle, in linea con quanto suggerito: • dalle linee guida AGID; • dalle linee guida OWASP; • dalle linee guida SANS.	Documentazione/Procedure
RS35	**Application Domain**	Secure Code Review	Il servizio deve essere sottoposto ad attività periodiche di Secure Code Review al fine di individuare e mitigare potenziali vulnerabilità presenti nel codice applicativo. Tali attività devono essere svolte con cadenza almeno annuale e comunque a fronte di ogni nuovo rilascio o major change che impattino il servizio. I report relativi alle attività di Secure Code Review devono essere condivisi con il Committente.	Documentazione/Procedure
RS36	**Application Domain**	Patch Management	Su ciascun server fisico o istanza virtuale o componente applicativa installata è necessario che: • sia valutata l'opportunità o la necessità di installare le patch (es. hotfix, etc.) segnalate dai relativi Vendor e/o mediante l'attività di verifica periodica dello CSIRT Puglia; • le scelte sulle patch da installare siano attentamente valutate in modo da evitare eventuali problemi di compatibilità con altri programmi installati sullo stesso server o su altri server con cui deve sussistere un flusso di dati informatici; • le scelte di non applicare una determinata patch (o un insieme di patch) siano condivise per approvazione con il Committente e con lo CSIRT Puglia, esplicitando le motivazioni della non installazione e indicando gli eventuali rischi informatici derivanti da tale scelta; • siano svolti esaustivi test di compatibilità per accertare sia la compatibilità che le eventuali modifiche (relative alle impostazioni di rete e sicurezza) da apportare alle preesistenti configurazioni nel caso in cui il Vendor non rilasci sufficienti informazioni o garanzie di	Documentation/Procedure

ID	Dominio	Argomento	Requisito	Tipologia
			compatibilità con altri programmi installati sullo stesso server; • il livello di patching sia mantenuto adeguato attraverso il continuo aggiornamento e in ogni caso prima della messa in produzione; • sia disponibile fuori linea la gold copy del software standard da installare sulle diverse tipologie di server e componenti applicative opportunamente aggiornato; • la manutenzione del patching dei programmi sia gestita, ove possibile, in maniera automatizzata mediante l'uso di un software che permetta di monitorare lo stato dei sistemi (ad esempio attraverso l'utilizzo di un servizio di EarlyWarning) e il loro allineamento all'ultimo livello di patch; • la manutenzione dei sistemi sia effettuata evitando il degrado delle prestazioni di banda delle reti e dei servizi impattati; • la gestione del servizio consenta la possibilità di scegliere/impostare un determinato livello di patching per un gruppo di ambienti (es. server, database, application server, etc.).	
RS37	**Application Domain**	Decomissioning	Al termine dello sviluppo di una funzionalità e/o di un modulo applicativo, tutti gli ambienti di sviluppo e di test del software devono essere adeguatamente dismessi. Tutte le informazioni devono essere archiviate e cancellate in modo sicuro in base ai requisiti normativi.	Documentation/Procedure

Tabella 8: Tabella dei Requisiti di Sicurezza (RS) relativi all'Application domain

Monitoring domain

Il monitoring and response domain consente di loggare e monitorare servizi e risorse al fine di ricevere avvisi di sicurezza o incidenti a seconda delle policy e delle soglie impostate. Il monitoraggio aiuta anche a predisporre una risposta automatica ai principali problemi di sicurezza afferenti al mondo cloud.
Di seguito l'elenco dei requisiti identificati per questo dominio:

ID	Dominio	Argomento	Requisito	Tipologia
RS38	**Monitoring Domain**	Log Generation	Tutte le componenti del servizio devono prevedere la possibilità di generare log di audit, funzionali, di sicurezza e di privacy al fine di garantire visibilità su tutte le attività	Configurazione

ID	Dominio	Argomento	Requisito	Tipologia
			svolte. Tali log devono contenere a titolo esemplificativo e non esaustivo informazioni quali: timestamp, utente, sistemi coinvolti (sorgente e destinazione), descrizione dell'attività svolta, etc. Per ogni tipologia di log deve essere possibile definire un opportuno periodo di retention all'interno del servizio.	
RS39	**Monitoring Domain**	Log Gathering	Il servizio deve consentire l'interfacciamento con soluzioni di Log Management/SIEM e consentire l'invio dei log generati attraverso l'utilizzo di protocolli e formati standard (es. Syslog, CEF, LEEF, etc.) usando una logica di streaming delle informazioni in real-time o near real-time. Indipendentemente dalla disponibilità di un proprio SIEM, al fornitore potrà essere richiesto di interfacciare e condividere log con il SIEM gestito dal CSIRT Puglia.	Configurazione
RS40	**Monitoring Domain**	Resource Monitoring	È necessario attivare la funzione di monitoring delle risorse all'interno dell'istanza del Cloud Service Provider per identificare potenziali malfunzionamenti e anomalie.	Technology/Technical control
RS41	**Monitoring Domain**	Security Incident Management	In ambito "*Security Incident Management*" viene richiesto al Fornitore di: • monitorare tutte le infrastrutture gestite, su tutti gli incidenti di sicurezza. Nello specifico è richiesto al Fornitore di valutare la portata di un eventuale incidente di sicurezza in termini di impatto rispetto ai dati personali e all'erogazione dei servizi; • fornire una reportistica dettagliata di tutti gli eventi con report aggregati e di dettaglio; • fornire una reportistica dettagliata sui servizi impattati dall'incident di sicurezza; • gestire l'implementazione delle remediation indicate. Lo CSIRT Puglia dovrà essere sempre interessato in caso di incidenti, previa registrazione a cura del fornitore sul portale CSIRT https://csirt.puglia.it	Documentation/Procedure

ID	Dominio	Argomento	Requisito	Tipologia
RS42	**Monitoring Domain**	SIEM	Il fornitore deve prevedere l'implementazione, la configurazione e la gestione di una soluzione di *Security Incident and Event Management* al fine di raccogliere i log prodotti, individuando le sorgenti di log rilevanti da un punto di vista security e di compliance, e di effettuare le opportune correlazioni sugli stessi al fine di intercettare potenziali fenomeni malevoli. I sistemi di raccolta, elaborazione e archiviazione dei log devono essere sincronizzati con una Time Source affidabile e comune (NTP). Indipendentemente dalla disponibilità di un proprio SIEM, al fornitore potrà essere richiesto di interfacciare e condividere log con il SIEM gestito dal CSIRT Puglia	Technology/Technical control

Tabella 9: Tabella dei Requisiti di Sicurezza (RS) relativi al Monitoring domain

Si conferma che lo CSIRT Puglia effettuerà dei controlli periodici volti per identificare eventuali vulnerabilità all'interno delle applicazioni in fase di esecuzione e l'analisi dell'esposizione al rischio di attacchi informatici ai sistemi informativi mediante l'utilizzo di tecniche di analisi statica e dinamica ed attraverso l'esecuzione di Vulnerability Assessment e Penetration Test. Il Fornitore sarà obbligato ad attuare tutte le contromisure e i piani di rientro necessari a correggere le vulnerabilità riscontrate dai controlli eseguiti.

Response domain

Di seguito l'elenco dei requisiti identificati per il response domain:

ID	Dominio	Argomento	Requisito	Tipologia
RS43	**Response Domain**	Backup and Restore	Per garantire una corretta protezione degli apparati e delle soluzioni di sicurezza, il servizio deve prevedere una procedura di backup & restore delle configurazioni e delle soluzioni di sicurezza. Il Fornitore deve eseguire test periodici afferenti alle procedure di backup&restore dandone evidenza al Committente.	Configuration

Tabella 10: Tabella dei Requisiti di Sicurezza (RS) relativi al Response domain

Assunzioni

In ambito sicurezza, per l'implementazione della nuova CCE, sono da ritenersi valide le seguenti assunzioni:
È in carico al Fornitore la verifica di eventuali impatti derivanti dall'implementazione dei presidi di sicurezza indicati sulle prestazioni della CCE.
Sono in carico al Fornitore i costi di licenza delle soluzioni tecnologiche che verranno implementate al fine di rispettare i requisiti di sicurezza descritti.

Sono in carico al Fornitore l'implementazione, la configurazione e la gestione di tutte le soluzioni tecnologiche di sicurezza menzionate nei requisiti.
Si precisa che i dati personali trattati non dovranno essere trasferiti al di fuori dell'Unione Europea.

Data Breach

A seguito dell'evento di violazione o potenziale violazione, rispettando i limiti temporali di notifica al Garante da parte del Titolare entro le 72 ore dalla scoperta dell'evento, la Ditta Appaltatrice deve produrre una relazione contenente tutti gli elementi necessari per valutare se la violazione di sicurezza ha comportato, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.
La relazione deve, altresì, accertare se la violazione dei dati personali ha compromesso la riservatezza, l'integrità o la disponibilità di dati personali e se la stessa ha comportato un rischio per i diritti e le libertà delle persone fisiche.
A tal fine la relazione deve descrivere le cause del malfunzionamento, le numeriche dei dati/utenti impattati, le misure correttive adottate di risoluzione del malfunzionamento con relative tempistiche, le misure volte alla mitigazione del rischio da possibili violazioni future nonché tutte le informazioni necessarie al titolare del trattamento per la notifica all'autorità Garante.

Si precia che a valle della stipula del Contratto Esecutivo verrà fonito il documento che descrive il flusso di notifica delle violazioni dei dati personali che presentano un rischio per i diritti e le libertà delle persone fisiche (Data Breach) in conformità a quanto previsto dal Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016.
La Ditta Appaltatrice deve garantire, nell'ambito della conduzione del sistema, quanto sopra esposto nel rispetto della normativa vigente ed in particolare:

- artt. 33 e 34 Regolamento (UE) n. 2016/679 (GDPR);
- Linee Guida dell'European Data Protection Board (EDB) del 14-01-2021;
- Deliberazione di Giunta n. 1905 del 19/12/2022 "Procedura per la gestione degli eventi di violazione dei dati personali (c.d. Data breach) ai sensi degli artt. 33 e 34 Regolamento (UE) n. 2016/679 (GDPR).

8 GARANZIA

Ogni prodotto software realizzato/modificato dal fornitore deve essere pienamente rispondente ai requisiti funzionali espressi, ai requisiti non funzionali (come indicati dalle norme ISO 25000 SQuaRe), alla Roadmap di migrazione al Cloud dell'Amministrazione, nonché agli standard, linee guida di cui al paragrafo 8.10 del CTS Lotti Applicativi.
Eventuali anomalie, difettosità residua e incongruenze su basi dati, flussi, output erroneamente prodotti per effetto o propagazione dei malfunzionamenti devono essere rimosse, come parte integrante dei servizi che li hanno realizzati, a totale carico del fornitore, senza alcun pagamento da parte dell'Amministrazione.
La garanzia comporta, dunque, la correzione gratuita dei difetti riguardanti:

- gli oggetti software nuovi e/o modificati;
- le basi dati / flussi dati/ output deteriorati come ripercussione dei difetti;
- la documentazione, obbligatoriamente associata al software, in conformità ai requisiti di accuratezza, comprensibilità, consistenza e completezza.

Le suddette garanzie devono essere prestate in proprio dal fornitore anche per il fatto del terzo, intendendo l'Amministrazione restare estranea ai rapporti tra il fornitore stesso ed il terzo.
I tempi di ripristino devono rispettare l'indicatore "TRCG – Tempestività di Ripristino dell'Operatività in collaudo ed in garanzia" (cfr. appendice Livelli di Servizio).

Garanzia durante l'erogazione
La garanzia si applica, per tutta la durata dell'erogazione dei servizi realizzativi e correttivi, su tutto il software modificato/integrato per i seguenti servizi, fatto salvo quanto previsto dal Capitolato Tecnico Speciale al paragrafo

5:

- servizi di manutenzione Evoluzione Applicazioni Esistenti
- servizi di Manutenzione Adeguativa e Migliorativa;

Come già indicato, tale software non potrà mai essere conteggiato nella Manutenzione Correttiva Software Pregresso.

Garanzia Post-erogazione

Al termine del contratto il fornitore risponde della difettosità dopo la verifica di conformità per massimo 12 mesisul software da esso modificato e realizzato. Il vincolo di garanzia è valido se il software non viene modificato dal fornitore subentrante.

9 CLASSI DI RISCHIO DELLE APPLICAZIONI

La classe di rischio di un'applicazione, e di conseguenza le attività che insistono sull'applicazione stessa, è definita come segue:

- Classe A: l'applicazione o una sua funzionalità o il progetto sono caratterizzati da una elevatissima criticità- dovuta alle possibili responsabilità civili e/o economiche e/o penali e dal loro potenziale impatto sull'esterno, connesse alla importanza economica e sociale dei dati acquisiti o elaborati, dai servizi offerti al cittadino/impresa/parti sociali/enti nazionali ed internazionali. Il ritardo nell'attivazione anche di una sola funzionalità e/o malfunzionamenti e/o l'indisponibilità temporanea del servizio può provocare danni gravi e diffusi verso terzi oppure causare una consistente perdita di immagine dell'Amministrazione e di fiducia verso i servizi da essa offerti al cittadino/impresa, ad altre Amministrazioni e verso l'esterno. A titolo di esempio rientrano in questa categoria progetti realizzativi collegati a finanziamenti che possono comportare la riduzione e/o la perdita anche parziale del contributo; progetti e attività collegate a servizi informatici a supporto di processi amministrativi vincolati per legge; processi informatici a supporto di servizi di emergenza (es. 112).
- Classe B: l'applicazione od una sua funzionalità o il progetto sono caratterizzati da limitate responsabilità civili e/o penali dovuta e limitato impatto potenziale sull'esterno. Il ritardo nell'attivazione anche di una sola funzionalità e/o malfunzionamenti e/o l'indisponibilità temporanea del servizio può provocare un contenuto danno di immagine e/o economico dell'Amministrazione, recuperabile in tempi brevi. Eventuali perdite di dati riservati e/o sensibili è limitata nel tempo e nell'entità senza causare danni ai cittadini/imprese e altre Amministrazioni nazionali ed internazionali.
- Classe C: l'applicazione od una sua funzionalità o il progetto implicano la gestione di informazioni non critiche; un eventuale malfunzionamento comporta la sola perdita del lavoro svolto, o danni di limitato valore economico.

10 ATTIVITÀ PROPEDEUTICHE ALL'EROGAZIONE DEI SERVIZI

Il fornitore deve garantire il pieno rispetto dei requisiti minimi e dei livelli di servizio a partire dalla data di stipula. In questo ambito trovano applicazione le regole relative agli indicatori di qualità riportati dell'Appendice Livelli di Servizio.

Obbligo del fornitore

Il Fornitore aggiudicatario dovrà garantire l'esecuzione della fornitura a regola d'arte attraverso il pieno rispetto dei requisiti minimi e dei livelli di qualità di servizio a partire dalla data di inizio attività e garantire l'efficacia dei servizi dall'avvio della fornitura.

Il Fornitore deve inoltre garantire che ogni dimensionamento dei servizi sia rispondente all'effettivo *effort* impiegato ed impiegabile: sopravvalutazioni, conteggi di attività non eseguite o non necessarie od in garanzia determinano un danno erariale e comportano la risoluzione immediata ed in danno dell'AS. Il fornitore dovrà

impiegare personale qualificato nel dimensionamento delle attività applicative, realizzare procedure e meccanismi di controllo per garantire la trasparenza ed onestà dell'impresa.

Attività propedeutiche all'erogazione dei servizi

Il Fornitore aggiudicatario dovrà prevedere tutte le attività preparatorie alla presa in carico dei servizi, acquisendo il know-how sul contesto tecnologico e applicativo nonché di processo e organizzativo della fornitura, predisporre gli ambienti tecnologici e/o strumenti operativi e di supporto necessari per l'erogazione della fornitura.
Tutte le spese e gli oneri del Fornitore, relativi alle attività propedeutiche all'erogazione del servizio oggetto del presente Appalto Specifico, sono da intendersi ricomprese e compensate nel corrispettivo complessivo della fornitura.

Presa in carico

A partire dalla stipula del Contratto esecutivo il fornitore dovrà acquisire gli standard, linee guida e metodologie in uso presso l'Amministrazione, predisporre i collegamenti telematici e di rete con l'Amministrazione, configurare il Portale della Fornitura per il Contratto Esecutivo, acquisire i dati di gestione e di baseline, predisporre e configurare gli strumenti tecnologici richiesti e offerti per garantire l'operatività dei servizi, l'efficacia delle comunicazioni e l'efficienza dei processi.
Il fornitore dovrà prevedere la rilevazione degli indicatori di digitalizzazione indicati nel Capitolato tecnico parte generale paragrafo 9.2 relativamente ai servizi richiesti.
Tutte le attività di Presa in carico dovranno essere avviate entro 15 giorni dalla stipula del contratto ed eseguite secondo le tempistiche concordate con l'Amministrazione nel Piano di Presa in carico e Subentro. Le scadenze sono presidiate dall'indicatore "RSCT – Rispetto di una scadenza contrattuale" dell'Appendice Livelli di Servizio. Il servizio di presa in carico e acquisizione di know how è inteso a totale carico dell'aggiudicatario e pertanto non comporterà oneri aggiuntivi per l'Amministrazione.
L'attività di presa in carico iniziale dovrà essere effettuata entro il termine massimo di due mesi solari dalla data di stipula del contratto esecutivo.

Subentro

Il subentro è finalizzato alla presa in carico del parco applicativo esistente, comprensivo di tutti gli strumenti e della documentazione di supporto e di eventuali obiettivi e progetti già definiti dall'Amministrazione.

Il periodo di addestramento iniziale è stimato in un massimo di due mesi (c.d. Subentro Complesso come da CTS Lotti Applicativi par. 7.4), da definire nel Piano di Subentro in funzione di eventuale know-how già disponibile da parte dell'aggiudicatario.

Tale addestramento potrà consistere, ad esempio, in riunioni di lavoro, esame della documentazione esistente con assistenza
di personale esperto, affiancamento nell'operatività quotidiana condotta dal fornitore uscente o esecuzioni di verifiche preventive su procedure critiche, illustrazione dell'attuale livello di qualità del software con dettaglio delle non conformità, violazioni, grado di riuso del software, ecc.
Durante le attività di subentro la responsabilità dei servizi continuerà ad essere in capo al fornitore uscente. Nel periodo di subentro il fornitore deve:

- redigere il piano di implementazione delle eventuali soluzioni migliorative dichiarate in offerta tecnica;
- produrre la documentazione relativa alle modalità di misurazione degli Indicatori di Qualità. L'Amministrazione potrà richiedere che tale documentazione venga redatta su appositi template appositamente forniti;
- Per i servizi di manutenzione:

- svolgere l'Assessment della qualità del software in questione, in particolare della manutenibilità e la presenza di vulnerabilità;
- eseguire attività di raccolta dati di difettosità e di assistenza sul software in esercizio;
- acquisire i Piani di lavoro del fornitore uscente con il dettaglio dei ticket e delle richieste di assistenza; acquisire eventuali basi dati di conoscenza e classificazione delle attività, già esistenti presso l'Amministrazione, per ottimizzare i tempi e la qualità delle risposte.

Durante lo svolgimento di queste attività, il Fornitore dovrà completare il conteggio in PF della baseline di partenza, dandone evidenza all'Amministrazione attraverso apposita documentazione. Si precisa che per baseline si intende tutto il patrimonio software dell'Amministrazione, costituito sia da software in garanzia (che non contribuisce al calcolo del canone della MAC), sia dal software non in garanzia, da cui invece scaturisce il calcolo del canone della MAC.

Il Fornitore dovrà quindi garantire:

- le relazioni di avanzamento, supportate da strumenti che facilitino la comunicazione ed il monitoraggio puntuale delle attività e il presidio dei fattori di rischio; in caso di criticità, mancato supporto del Fornitore uscente, documentazione incompleta, software non commentato, mancato rispetto della tempistica, il responsabile del Fornitore dovrà inviare immediatamente una comunicazione (anche via posta elettronica) esplicitando le azioni di recupero (se nella propria disponibilità) o le attività bloccate affinché l'Amministrazione possa intervenire;
- la presenza di tutte le figure necessarie alla presa in carico dei servizi ed il presidio delle attività di subentro; in particolare, durante lo svolgimento attività di subentro, dovranno essere reperibili e disponibili i Responsabili Tecnici per l'erogazione dei servizi;
- la partecipazione dei professionisti coinvolti nella presa in carico a tutti gli incontri di allineamento, formazione, training on the job previsti dal piano; le modalità di fruizione e la pianificazione di tale addestramento dovranno essere concordate con l'Amministrazione, anche sulla base di eventuali proposte che il Fornitore effettuerà nell'Offerta Tecnica;
- la presenza ed il mantenimento nel tempo delle percentuali di personale con le certificazioni e/o credenziali dichiarate in offerta tecnica valide e non scadute;
- la predisposizione di un verbale attestante il completamento del passaggio di consegne, da redigere secondo le indicazioni che l'Amministrazione fornirà all'atto della stipula del Contratto esecutivo e che dovrà essere sottoscritto dal Fornitore subentrante e dal Fornitore uscente e consegnato all'Amministrazione. Tale verbale dovrà indicare eventuali carenze della documentazione fornita a supporto del subentro, in termini di obsolescenza o incompletezza;
- il rispetto delle modalità e dei livelli qualitativi offerti per il subentro.

Le attività di subentro dovranno essere eseguite dal Fornitore su richiesta dell'Amministrazione Contraente entro le tempistiche dalla stessa indicate, pena l'applicazione della penale di cui al paragrafo 4.1.1 e 4.2.1 dell'Appendice Livelli di Servizio.
Tutte le attività di subentro sono senza oneri aggiuntivi per l'Amministrazione.
Durante le attività di subentro e sino alla data di attivazione definita nel Contratto esecutivo, la responsabilità dei servizi e di tutte le attività continuerà ad essere in capo al Fornitore uscente; in tale periodo, il Fornitore aggiudicatario non percepirà alcun corrispettivo. Per tutte le attività di subentro, l'Amministrazione si riserva di indicare ulteriori requisiti minimi in funzione dell'evoluzione del contesto applicativo e di esigenze attualmente non pianificabili o non prevedibili. Gli adempimenti sopra indicati, nonché quelli migliorativi eventualmente offerti, costituiscono requisiti minimi delle attività propedeutiche all'attivazione dei servizi.

Presentazione del Team da impiegare nell'affidamento

Si rimanda a quanto specificato nel CTS Lotti Applicativi par. 7.6 "Team da impiegare nell'affidamento".

Attività di fine fornitura

Il Fornitore dovrà predisporre un piano di qualità e un Piano di trasferimento per le attività di passaggio di consegne di fine fornitura (*phase-out*) con il trasferimento all'Amministrazione o a terzi da esso indicati, del *knowhow* e delle

competenze maturate nella conduzione dei servizi oggetto dell'Accordo Quadro e dei Contratti esecutivi.
Il passaggio di consegne di fine fornitura dovrà essere erogato dal Fornitore nel corso degli ultimi due mesi di vigenza contrattuale dell'Accordo Quadro, secondo la pianificazione concordata, senza oneri aggiuntivi per l'Amministrazione, in accordo con i requisiti di qualità indicati nel presente capitolato. Inoltre il Fornitore dovrà prevedere la disponibilità di un apposito gruppo di lavoro dedicato, con un numero consistente ed adeguato di risorse professionali, strumenti organizzativi e tecnologici, anche in relazione a quanto ulteriormente richiesto dall'Amministrazione e previsto in sede di offerta tecnica dal Fornitore.
Si fa presente che il trasferimento di know-how potrà essere richiesto anche durante l'erogazione dei servizi nel corso della durata contrattuale ed erogato direttamente al personale dell'Amministrazione.
Sono incluse nelle attività di trasferimento:

- il supporto all'Amministrazione nella definizione della progettazione di dettaglio delle attività
- (predisposizione piano di trasferimento, revisione documenti, ecc.);
- lo svolgimento delle attività di propria pertinenza in conformità alla pianificazione definita;
- il coordinamento generale e la supervisione delle attività di trasferimento di tutti gli attori coinvolti;
- il supporto e il monitoraggio continuativo, per tutta la durata delle attività di trasferimento, a tutti gli attori coinvolti per lo svolgimento delle attività;
- la produzione di report durante l'erogazione del servizio ed a conclusione della attività svolte per il trasferimento.

Di seguito si riportano i vincoli previsti nell'ambito del trasferimento:

- durata massima delle attività di trasferimento: due mesi solari continuativi dalla data di avvio del Trasferimento che sarà indicata dall'Amministrazione. Per tutta la durata del trasferimento il Fornitore erogherà i servizi di propria pertinenza; a partire dal primo giorno successivo al collaudo del generico servizio contrattuale (o parte di esso) il Fornitore subentrante subentrerà nella sua gestione al Fornitore, il quale continuerà a garantire la sua assistenza sui prodotti software realizzati e sui servizi erogati secondo quanto previsto dalle specifiche contrattuali.
- modifiche architettura tecnologica: non sono ammesse modifiche agli ambienti operativi e applicativi gestiti.
- Predisposizione del Piano di trasferimento: Il Piano di trasferimento (PTF) deve contenere il dettaglio delle attività, la relativa tempificazione e le stime di impegno e, in particolare, i seguenti contenuti minimi:
  - l'oggetto del trasferimento: presentazione esaustiva degli aspetti organizzativi, amministrativi e tecnici della fornitura, dei processi di riferimento, dell'architettura generale del sistema nonché delle architetture di ogni singola applicazione;
  - le attività e le relative modalità di esecuzione;
  - modalità di estrazione, verifica e consegna di tutti gli oggetti software al fine di permettere la predisposizione di un ambiente operativo parallelo;
  - i compiti e le responsabilità di ciascuna delle Parti;
  - il programma temporale in base al quale le attività dovranno essere eseguite;
  - l'analisi dei rischi per la continuità dei servizi dell'Amministrazione;
  - le contromisure da adottare per far fronte ai rischi individuati;
  - presentazione degli aspetti di criticità di ogni servizio/applicazione con l'esposizione chiara delle soluzioni proposte ed attuate durante la fornitura;
  - i piani di collaudo dei servizi oggetto di trasferimento.

Il PTF sarà redatto dal Fornitore e sottoposto all'approvazione dell'Amministrazione almeno tre mesi prima della scadenza dell'Accordo Quadro, ovvero entro i due mesi successivi alla data di comunicazione dell'evento che ne comporterà la cessazione anticipata. Il documento prodotto dovrà essere gestito dal Fornitore ed aggiornato a seguito delle modifiche richieste dall'Amministrazione ovvero intervenute nel corso di svolgimento delle attività di trasferimento (ad esempio a seguito del riesame congiunto con il Fornitore subentrante nella fase di trasferimento o anche successivamente durante lo svolgimento delle attività di trasferimento per aggiunta/modifica o cancellazione di
attività/riunioni). Il piano di trasferimento dovrà prevedere, per le fasi di passaggio della conoscenza e verifica, l'effettuazione di sessioni di lavoro nelle quali i rappresentanti del Fornitore e del Fornitore Subentrante

esamineranno congiuntamente la documentazione relativa agli oggetti da trasferire. Le sessioni costituiscono raggruppamenti omogenei di riunioni (collegati ad un'unica area tematica – es. servizio xyz, area applicativa, ecc.). Al termine di ogni riunione sarà redatto l'apposito verbale dal Fornitore, mentre al termine dell'ultima riunione di ogni sessione viene redatto un verbale di fine
sessione. Tale verbale riepiloga le questioni che non hanno trovato soluzione nell'ambito delle riunioni tecniche, e viene trasmesso alle riunioni di SAL per la verifica ed il riesame dei problemi aperti e la chiusura formale delle sessioni. Il piano conterrà anche il programma di dettaglio delle singole riunioni relative a tutte le fasi del progetto di trasferimento.
Nella redazione del PTF occorre tener conto delle priorità relative alle scadenze istituzionali dell'Amministrazione e delle concatenazioni degli adempimenti tecnico amministrativi, secondo le priorità dall'Amministrazione stessa.
La responsabilità di ciascun servizio verrà mantenuta dal Fornitore fino al termine delle attività di trasferimento del servizio specifico (o parte di esso) in conformità con quanto previsto dal PTF.
Rientra nelle responsabilità generali del Fornitore anche:

- il coordinamento generale di tutti gli attori coinvolti e la supervisione delle attività di trasferimento;
- il supporto, per tutta la durata delle attività di trasferimento, a tutti gli attori coinvolti per lo svolgimento
- delle attività;
- il project management generale del progetto;
- il reporting delle attività svolte al termine del trasferimento.

Le attività saranno svolte sulla base del PTF, predisposto sulla base dell'integrazione con il Piano di subentro del Fornitore subentrante.

Si fa presente che il trasferimento di know-how potrà essere richiesto anche nel corso della fornitura.
Il Fornitore, nel corso delle attività di trasferimento, dovrà rispondere a qualsiasi quesito in merito ai sistemi gestiti per consentire il trasferimento di conoscenza al nuovo Fornitore. Allo scopo dovrà rispondere entro 2 giorni lavorativi da ogni richiesta dell'Amministrazione o delle terze parti designate, mediante la consegna di una Scheda Informazioni, in cui siano riportate:

- la/e richiesta/e dell'Amministrazione o delle terze parti designate con l'indicazione delle specifiche degli output attesi (sia in termini di contenuti che di formati);
- la risposta del Fornitore circa la/e richiesta/e dell'Amministrazione o delle terze parti designate comprensiva delle informazioni necessarie all'uso degli output delle risposte;
- gli allegati alla scheda informazioni (output delle richieste).

Unitamente alle schede informazioni saranno consegnati tutti gli output necessari al soddisfacimento della richiesta dell'Amministrazione o delle terze parti coinvolte: la mancata consegna degli output richiesti comporterà l'applicazione delle sanzioni previste.
Infine, entro 15 giorni lavorativi dal termine delle attività di trasferimento il Fornitore dovrà predisporre un Rapporto finale di trasferimento, nel quale siano esplicitate, per ogni attività prevista nel Piano di trasferimento:

- la data di avvio prevista ed effettiva;
- la data di conclusione prevista ed effettiva;
- la descrizione delle attività svolte da tutti gli attori coinvolti;
- l'elenco dei problemi rilevati (oggetto, data rilevazione problema, criticità, impatti, responsabile per la risoluzione) e le azioni messe in atto per la risoluzione, con l'indicazione della data di risoluzione prevista ed effettiva.

Le informazioni riportate dovranno essere aggiornate ai 5 giorni solari antecedenti la data di consegna del Rapporto.
In tale rapporto dovranno inoltre essere presenti:

- le rendicontazioni degli indicatori di qualità;
- le rendicontazioni di dettaglio degli effort erogati per ciascuna attività prevista dal piano del trasferimento con il dettaglio di: a) Nominativo (nome e cognome); b) Profilo professionale; c) Effort in gg/persona erogato per ogni attività in cui la risorsa è stata coinvolta; d) Descrizione dell'attività effettuata nell'ambito del piano.
- le rendicontazioni di sintesi degli effort erogati raggruppate per profilo professionale con l'indicazione delle tariffe applicabili;
- i verbali eventualmente redatti e sottoscritti dalle parti per ciascuna attività aggiuntiva svolta nei 2 mesi

successivi al termine del trasferimento.
Allo scopo il Fornitore dovrà registrare tutti gli effort delle risorse impegnate nelle attività di esecuzione del trasferimento per tutta la durata delle attività stesse. Tali registrazioni dovranno essere consegnate unitamente al rapporto finale per consentire le verifiche da parte dell'Amministrazione.

11 MODALITÀ DI EROGAZIONE

Comunicazioni e Approvazioni

I piani di Qualità ed i Piani di lavoro, ed in genere i documenti richiesti contrattualmente devono essere notificati formalmente. Per favorire l'agilità e la digitalizzazione dei processi – a partire da quelli interni di funzionamento dell'interazione con l'Amministrazione – il fornitore dovrà rendere disponibile sul Portale della fornitura una apposita funzione di validazione dei documenti e di approvazione da parte dell'Amministrazione.
Il relativo workflow di approvazione dei documenti dovrà essere definito nel Piano della Qualità Generale e reso disponibile nella Prima Release del Portale.
Si precisa che la mancata approvazione di documenti contrattuali (e/o artefatti di servizi) costituisce inadempimento contrattuale cui può conseguire l'adozione delle azioni contrattuali indicate dell'Accordo Quadro e nell'appendice Indicatori di Qualità.

Modalità di Approvazione dei Prodotti

Tutte le comunicazioni inerenti all'approvazione (o mancata approvazione) dei prodotti della fornitura saranno notificati tramite il Portale. In nessun caso l'approvazione potrà avvenire per tacito assenso.
Il fornitore dovrà aggiornare i prodotti soggetti a rilievi e/o mancata approvazione senza alcun onere aggiuntivo per la Amministrazione.
Per tutti i prodotti della fornitura soggetti ad approvazione, la presenza di anomalie di gravità tale da impedire lo svolgimento delle attività di verifica comporta l'applicazione delle sanzioni contrattualmente previste.
I prodotti della fornitura che sono soggetti ad approvazione formale sono: Piano della qualità generale, Piano di presa in carico, Piani di Qualità, Piani di lavoro di ciascun servizio, Piano di lavoro degli obiettivi realizzativi, Piano di lavoro degli interventi a corpo, Piano dei servizi continuativi, Piano di trasferimento di know-how, gli artefatti obbligatori per ciascun servizio salva differente indicazione dell'Amministrazione nel Piano di qualità. Si rimanda all'appendice "Cicli e Prodotti". I restanti prodotti sono sottoposti a controllo (Accettazione/Verifica e Validazione) da parte della Amministrazione, che pertanto potrà non accettarli e richiedere di apportare le modifiche ritenute necessarie.
In ogni caso, si precisa che le anomalie, intese come malfunzionamenti, disallineamenti, non corrispondenza ai requisiti dovranno essere risolte dal fornitore per permettere la prosecuzione delle attività, entro i tempi definiti dalla Amministrazione o dal Capitolato Tecnico e relative appendici. Eventuali ritardi nella risoluzione delle anomalie comporteranno l'applicazione delle sanzioni contrattualmente previste.
Per i servizi gestiti in modalità progettuale, nel caso si verifichino situazioni "anomale" che, a giudizio della Amministrazione, sia per numerosità sia per gravità, sia per non rispetto dei tempi massimi indicati dalla Amministrazione per la risoluzione delle difformità, non consentano lo svolgimento o la prosecuzione delle attività, la Amministrazione procederà alla sospensione delle verifiche di accettazione e lo slittamento del termine della fase stessa sarà a totale carico del fornitore comportando le azioni contrattuali previste. La consegna della versione corretta dei prodotti dovrà avvenire entro il nuovo termine fissato dalla Amministrazione.

Collaudo degli obiettivi realizzativi

Il collaudo sarà svolto dalla Amministrazione nei tempi previsti dal Piano di Lavoro, con il supporto del fornitore. Durante il periodo di collaudo saranno oggetto di collaudo tutti i prodotti della fase realizzativa e la loro coerenza con i prodotti delle fasi precedenti.

L'attività di collaudo verrà svolta negli ambienti (collaudo) della Amministrazione, secondo gli standard e gli indirizzi metodologici indicati dalla Amministrazione.
Qualora la Amministrazione riscontri che casi di test dichiarati positivi dal fornitore falliscono durante il collaudo, il fornitore dovrà motivare la situazione ed in ogni caso verrà applicata l'azione contrattuale indicata dell'Allegato "Livelli di Servizio".
La fase di collaudo verrà pianificata dalla Amministrazione in accordo con il fornitore. Le anomalie, i malfunzionamenti e le difformità con la documentazione dovranno essere tempestivamente risolti dal fornitore per permettere la prosecuzione delle attività di collaudo, entro comunque i tempi definiti dall'Allegato "Livelli di servizio" e/o dalla Amministrazione. Eventuali ritardi nella risoluzione dei malfunzionamenti comporteranno l'applicazione delle azioni contrattualmente previste.
Nel caso in cui le anomalie, malfunzionamenti, difformità o i ritardi nella risoluzione degli stessi, a giudizio della Amministrazione, siano tali da non consentire lo svolgimento o la prosecuzione delle attività di collaudo, quest'ultimo verrà dichiarato sospeso e l'eventuale slittamento del termine della fase sarà a totale carico del fornitore comportando le azioni contrattuali previste. La consegna della versione corretta dei prodotti oggetti di collaudo dovrà avvenire entro il nuovo termine fissato dalla Amministrazione.
La ripresa del collaudo decorrerà dalla consegna della versione corretta dei prodotti: in nessun caso potrà essere ripianificata la fine della fase di collaudo e quindi eventuali ritardi rispetto alla pianificazione precedente sono imputabili al fornitore e evidenziati nell'indicatore di qualità corrispondente.
Qualora il collaudo dia nuovamente esito negativo, l'Amministrazione si riserva la facoltà di dichiarare non approvabile il prodotto oggetto di verifica per inadempimento del Fornitore.
L'Amministrazione avrà altresì la facoltà di risolvere il contratto.
In caso di esito positivo del collaudo, l'Amministrazione redige e sottoscrive la lettera di accettazione, cui sarà allegato il documento Rapporto di collaudo in cui sono tracciate le attività svolte durante il collaudo stesso.

Rilevazione della Qualità della Fornitura

L'appendice livelli di servizio prevede indicatori oggettivi standardizzati per ciascun servizio e trasversali sui servizi (gestione della fornitura) richiesti obbligatoriamente dalla documentazione di gara e gli indicatori e KPI offerti dai fornitori che diventano – come tutta l'offerta tecnica – parte integrante del contratto.
L'indicatore di Qualità della Fornitura sarà a disposizione degli Organismi di Controllo e Monitoraggio, di Consip, e di tutte le Amministrazioni utilizzatrici effettive e potenziali dell'AQ.

Azioni contrattuali

INADEMPIMENTI

Ogni inadempimento contrattuale darà origine ad un'azione commisurata alla criticità dell'inadempimento stesso. I principali aspetti delle prestazioni contrattuali vengono presidiati da appositi indicatori di qualità. Altri aspetti non sono oggetto di misurazioni strutturate di cui all'appendice "Livelli di servizio", ma, per disservizi ritenuti gravi, vengono direttamente presidiate nel capitolato tecnico e/o nel contratto.
Il mancato rispetto dei requisiti minimi richiesti e/o migliorati dal fornitore in Offerta tecnica determina azioni contrattuali per il ripristino delle situazioni fuori soglia o fuori controllo, che possono consistere in una o più delle seguenti azioni:

- coinvolgimento di un livello più elevato di interlocutori sino agli Organismi tecnici di coordinamento e controllo (attivazione di una procedura di escalation);
- ripetizione da parte del fornitore dell'erogazione di una prestazione, rifacimento di una attività, riconsegna di un prodotto (chiusura di una non conformità);
- esecuzione di una azione correttiva sulle modalità di erogazione del servizio;
- applicazione di rilievi;
- perdita della quota variabile del corrispettivo legato al raggiungimento di un livello di qualità minimo;
- applicazione di penali;
- azioni aggiuntive (richiesta danni, risoluzione anticipata del contratto, ecc.) laddove previsto contrattualmente.
- Segue un approfondimento degli istituti a tutela della qualità dell'erogazione della fornitura.

RILIEVI

I rilievi sono le azioni di avvertimento da parte della Amministrazione conseguenti il non rispetto delle indicazioni

contenute nella documentazione contrattuale. Pertanto oltre a quanto esplicitamente previsto potrà essere emesso un rilievo su qualunque inadempimento se non diversamente sanzionato.
I rilievi non prevedono di per sé l'applicazione di penali, ma costituiscono avvertimento sugli aspetti critici della fornitura e, se reiterati e accumulati, danno luogo a penali, secondo quanto previsto in appendice "Livelli di Servizio".
I rilievi possono essere emessi dal Direttore dell'esecuzione della Amministrazione, dai responsabili di progetto e/o di servizio della Amministrazione e/o da strutture della Amministrazione preposte o di supporto al controllo e/o monitoraggio della fornitura e sono formalizzati attraverso una nota di rilievo, ognuna delle quali potrà contenere uno o più rilievi.
Qualora il fornitore ritenga di procedere alla richiesta di annullamento del rilievo dovrà sottoporre alla Amministrazione un documento con elementi oggettivi ed opportune argomentazioni entro 3 giorni lavorativi dall'emissione del rilievo.

INDICI DI PRESTAZIONE

Nell'appendice "Livelli di Servizio" sono descritti gli specifici indici di prestazione applicabili alla fornitura cui è legata una quota del corrispettivo maturato.
Gli indici di prestazione sono legati al raggiungimento delle soglie previste per uno o più indicatori di qualità come indicato nell'appendice stessa.
Gli indici di prestazione prevedono quote sospese distinte e disgiunte, pertanto il raggiungimento della soglia relativa al singolo indicatore collegato all'Indice di prestazione comporta la perdita della relativa quota sospesa, indipendentemente dagli altri indicatori.
Nel caso in cui il fornitore in sede di offerta proponga miglioramenti dei valori di soglia, siano essi legati ad indicatori di qualità generale che ai livelli di servizio, tali nuovi valori saranno assunti come nuovo profilo della qualità. In tal caso i valori di soglia degli indici di prestazione saranno adeguati a tale nuovo profilo.
Il raggiungimento della soglia degli Indici di prestazione sarà certificato attraverso apposita verifica di conformità.

PENALI

Lo scopo delle penali è riequilibrare il servizio effettivamente ricevuto (di minore qualità, e/o generando disservizi e/o ritardi e/o inducendo un danno all'utilizzatore) dalla Amministrazione al corrispettivo da erogarsi che è stabilito per prestazioni effettuate nel rispetto dei requisiti.

Monitoraggio

Le attività di monitoraggio dovranno essere conformi a quanto previsto dalla Circolare AgID n. 1 del 20 gennaio 2021 emessa dall'AgID.
La funzione di monitoraggio sarà svolta dalla Amministrazione o da soggetto da essa incaricato. Il fornitore si impegna a fornire all'Amministrazione tutti i documenti necessari all'attività di monitoraggio nei formati richiesti e necessari per il controllo e la verifica della fornitura, salvo evoluzioni derivanti dall'introduzione, da parte della Amministrazione, di strumenti automatici a ciò deputati.
Il fornitore si impegna ad inviare alla Amministrazione la documentazione comprovante l'eventuale esito delle visite di sorveglianza della società di certificazione della qualità e/o il rinnovo della certificazione entro 1 mese dalla data della verifica. Inoltre, il fornitore e/o i subfornitori devono rendersi disponibili alle verifiche anche ispettive effettuate dalla Amministrazione tramite personale proprio o da terzi da essa incaricati, svolte nel rispetto di quanto prescritto dalla serie di norme EN ISO 19011:2003.

Pianificazione e Consuntivazione

Piano della Qualità

Il Piano della Qualità Generale è descritto nel Capitolato Generale paragrafo 7.1.1.
La struttura ed i requisiti minimi del Piano della Qualità Specifico di Contratto Esecutivo sono indicati nell'appendice Cicli e Prodotti. Il fornitore dovrà mantenere i propri Piani di qualità aggiornati allo stato della tecnologia, di automazione, misurazione e controllo.
Il fornitore può redigere un Piano di Qualità di Obiettivo per specializzare e definire puntuali integrazioni o modifiche al Piano di Qualità Specifico del Contratto Esecutivo.

Il RUAC è responsabile della piena applicazione ed aggiornamento del Piano di Qualità a qualunque livello: a partire dall'inizio della fornitura e con cadenza massima trimestrale deve riferire e pubblicare sul i Portale Rapporti sul rispetto del Piano di qualità della fornitura ed i Rapporti di conformità su tutti gli impegni assunti in offerta tecnica.

Piani di Lavoro

Il fornitore dovrà predisporre- con le tempistiche indicate nel Capitolato Tecnico Generale - e mantenere costantemente aggiornata la pianificazione di tutte le attività, con la seguente articolazione:

- Piano di lavoro generale comprensivo di:
  - piano di Presa in carico e subentro di inizio fornitura, pianificazione delle attività trasversali di carattere generale ad esempio: pianificazione delle attività di assicurazione della qualità;
  - piano di lavoro dei servizi a carattere continuativo che si estrinsecherà in un piano per ogni servizio tenendo in considerazione le risorse di servizio esteso e di reperibilità;
  - piano di lavoro per le attività a carattere progettuale;
- eventuali piani di lavoro obiettivo, da produrre con le modalità concordate di volta in volta con le singole Amministrazioni.

Si rimanda all'Appendice Cicli e Prodotti per la descrizione puntuale dei contenuti dei suddetti piani, si precisa che, nell'ambito dei piani per i servizi a carattere continuativo, il fornitore dovrà indicare nel dettaglio tutte le attività previste.

A fronte di ripianificazioni autorizzate dall'Amministrazione, il fornitore redigerà e pubblicherà sul Portale la versione aggiornata del Piano di lavoro.

Il fornitore è tenuto a comunicare - entro il giorno lavorativo successivo al verificarsi dell'evento - qualsiasi criticità, ritardo o impedimento che modificano il piano concordato e ad inviare una ripianificazione delle attività, aggiornando e ripubblicando sul Portale il relativo Piano di Lavoro.

In nessun caso potrà essere rivisto il Piano di Lavoro in seguito ad uno o più rilievi emessi su artefatti che costituiscono milestone di fine attività; si precisa che la mancata approvazione di documenti contrattuali e/o artefatti di servizi costituisce inadempimento contrattuale e si applica l'indicatore MAPP oltre a poter generale ritardi rispetto alle scadenze contrattuali.

In qualunque momento l'Amministrazione può richiedere la consegna del Piano di Lavoro. Questo dovrà contenere tutti gli aggiornamenti concordati.

Il Piano di Lavoro e le sue modifiche certificano ai fini contrattuali gli obblighi formalmente assunti dal fornitore, e accettati dall'Amministrazione, su misurazioni e tempi di esecuzione delle attività e sulle relative milestone.

Si precisa che il Referente per i servizi di Gestione del Portafoglio Applicativo, nel caso di servizi erogati a consumo presso l'Amministrazione, dovrà farsi carico della gestione del personale componente il gruppo di lavoro (ad esempio ferie, malattie, indisponibilità in genere) al fine di garantire la regolare presenza delle risorse nell'orario di servizio. Nel caso sia necessaria una sostituzione temporanea, il responsabile (o il referente) dovrà concordare con la Amministrazione le modalità più adeguate di sostituzione.

E' pertanto necessario che il fornitore organizzi, pianifichi e monitori il servizio in modo da rispettare i livelli di servizio esplicitati in Allegato "Livelli di servizio".

Stato Avanzamento Lavori

Il fornitore dovrà mantenere aggiornata la sezione relativa allo stato di avanzamento dei lavori contenuta nei Piani di Lavoro approvati, fornendo sulla base della tempistica di aggiornamenti definita nel Piano di Qualità e dalle necessità del singolo intervento o ciclo di vita, o su richiesta dell'Amministrazione, indicazioni sulle attività concluse ed in corso, esplicitandone la percentuale di avanzamento, su eventuali rischi/criticità/ritardi, su eventuali impatti dei rischi/criticità, su azioni di recupero e razionali dello scostamento, sulle attività in servizio esteso ed in reperibilità.

Per le attività progettuali, la frequenza minima di aggiornamento è di 2 settimane. Per le attività continuative, in condizioni di attività di gestione con limitata variabilità di richieste di assistenza, può essere sufficiente un aggiornamento mensile.

Consuntivazione

La consuntivazione delle attività svolte dovrà essere predisposta dal fornitore mensilmente nella sezione Stato Avanzamento Lavori di ciascun Piano di lavoro relativamente a ciascun servizio e, se richiesto per ciascun applicativo.

Il piano di lavoro per i servizi di carattere continuativo deve essere corredato dal Rendiconto Risorse.

L'Amministrazione si riserva di chiedere un dettaglio di tale Rendiconto distinto per le attività prestate in servizio

esteso ed in reperibilità.
La consuntivazione delle attività svolte con modalità progettuale dovrà essere evidenziata sia nei singoli piani di obiettivo sia nel piano riepilogativo evidenziando le fasi chiuse e riportando gli eventuali scostamenti rispetto alla pianificazione concordata.

Attività previste a corpo o a consumo

Attività previste a canone

Servizio di Parametrizzazione e Personalizzazione di Soluzioni di terze parti/open source/riuso (PP)

Descrizione Servizio di Manutenzione Adeguativa e Migliorativa (MAD)

Descrizione Servizio di Manutenzione Correttiva (MAC)

Servizi di gestione applicativi e basi dati (GAB)

Servizio di Conduzione Tecnica (CT)

Attività previste a consumo

Servizio di Manutenzione Evolutiva di Applicazioni Esistenti (MEV)

Supporto Specialistico (SS)

Supporto tecnologico (ST)

Service Control Room per Monitoraggio tecnico/applicativo

Orario di erogazione dei servizi

Il Servizio deve essere erogato secondo le modalità descritte nella seguente Tabella.

Servizi	Orario	Estensioni	Reperibilità
Conduzione Tecnica	Giorni Feriali 08:00 – 20:00 (senza interruzione)	Su richiesta, sino al completamento delle 24 ore	Sì: telefono di reperibilità e presenza on-site entro 1 ora per le restanti ore al di fuori degli orari di erogazione del servizio

Si precisa che il sabato è compreso nei giorni feriali.

Si precisa che “senza interruzione” significa che il servizio, nell’orario indicato, non deve mai essere lasciato scoperto, ma potrà essere previsto nel Piano di lavoro una differente capacità di risposta nell’arco temporale. La copertura temporale potrà essere differenziata per servizi e per specifici applicativi indicando le modalità nel piano di lavoro; per festività devono intendersi solamente le festività a carattere nazionale e le domeniche, salvo casi indicati dall’Amministrazione in cui non vi siano servizi attivi.

A parità di numero di ore di presidio, l’Amministrazione si riserva di chiedere variazioni agli orari sopra definiti in funzione delle esigenze operative delle Aziende Sanitarie e della Regione Puglia.

Obblighi Generali del Fornitore nell'esecuzione dei Servizi

I Fornitori devono garantire il rispetto dei requisiti sotto descritti e l'applicazione delle buone pratiche tecnologiche e metodologiche, e delle metodologie di lavoro, descritte nel presente paragrafo, nell'esecuzione di ciascuna attività della fornitura.

Requisiti Tecnologici, il fornitore dovrà:

- garantire l'interoperabilità mediante l'esposizione di API come definito anche dalle linee guida di AgID;
- garantire l'utilizzo di formati standard aperti, evitando l'utilizzo di formati proprietari;
- usare strumenti e framework di sviluppo aperti e diffusi;
- garantire la portabilità dell'applicativo tramite l'utilizzo di *stack* tecnologici indipendenti dalla piattaforma;
- garantire l'indipendenza dalla piattaforma degli applicativi tramite l'utilizzo di strumenti di
- containerizzazione come ad es. Docker e architetture che separino lo strato applicativo della piattaforma;
- garantire la riusabilità funzionale del software realizzato;
- garantire che, all'interno del team che erogherà il servizio, siano presenti nel caso di prodotti Open Source contributori alle Community di riferimento;
- partecipare a reti di competenze e sviluppi collaborativi quali ad esempio developers.it;
- garantire la compatibilità del software realizzato/modificato con il release/livello effettivo degli ambienti di collaudo/esercizio attivi al momento in cui il software sarà utilizzato.

<u>Requisiti di qualità</u>

Il fornitore dovrà:

- garantire la qualità del software rilasciato o modificato attraverso il superamento delle soglie di qualità, l'assenza di non conformità e violazioni per le caratteristiche/sotto caratteristiche attualmente previste dal modello ISO/IEC 25000 Software product Quality Requirements and Evaluation (SQuaRE) e successive modifiche ed integrazioni. Si richiamano in particolare ISO/IEC 25010, ISO/IEC 25022 sulla misurazione della qualità in uso, ISO/IEC 25023 sulla misurazione della qualità del software e del sistema, ISO/IEC 25024 sulla misurazione della qualità dei dati, integrate con parametri – soglie e metriche aderenti al contesto applicativo proposte dal fornitore, dall'Amministrazione, dagli Organismi tecnici di monitoraggio e controllo;
- per ogni Progetto realizzativo la predisposizione e l'esecuzione di un piano di test esaustivo sotto tutti gli aspetti funzionali e non funzionali è obbligo contrattuale, senza oneri aggiuntivi. I risultati dei test devono essere accessibili all'Amministrazione e su richiesta dagli Organismi Tecnici di monitoraggio e controllo.

<u>Requisiti relativi alla redazione della documentazione di progetto e di servizio</u>

Ogni attività richiesta e svolta del fornitore comporta l'obbligo di rilasciare la documentazione a supporto per garantire la piena verifica della rispondenza di quanto svolto rispetto ai requisiti espressi dall'Amministrazione nonché il pieno trasferimento di know how all'Amministrazione, agli organismi di governo dei contratti strategici, agli attori subentranti nel processo di evoluzione/manutenzione nel tempo. Il software realizzato/modificato dovrà essere documentato secondo gli standard dell'Amministrazione o in assenza secondo gli standard e best practices indicati dal fornitore nel Piano della qualità. Il livello di documentazione, in ogni caso, deve permettere l'efficiente ed efficace presa in carico del progetto e/o dei sistemi in esercizio da parte dell'Amministrazione o da terzi da essa delegati nonché la rapida e affidabile diagnosi dei malfunzionamenti rilevati sul software.

Il fornitore produrrà la documentazione, per l'utente, per gestione applicativa e sistemistica.

Ciascun fornitore sarà tenuto a fornire all'Amministrazione, in funzione del servizio che sarà chiamato ad eseguire, le seguenti rappresentazioni:

- delle scelte architetturali: decisioni di progettazione del software che soddisfano un requisito funzionale o non funzionale e che hanno un impatto significativo sull'architettura del sistema;
- delle decisioni relative al business: decisioni che rientrano nell'ambito più strategico dell'amministrazione o di un progetto specifico;
- delle scelte relative al codice: per facilitare la comprensione, la modificabilità, la risoluzione rapida di malfunzionamenti.

<u>Requisiti metodologici</u>

Al fornitore si richiedono competenze in merito a metodologie, tecniche, strumenti, standard e linee guida coerenti e riconducibili alle principali metodologie, quali a titolo indicativo e non esaustivo:

- ISO 9000 che raggruppa le norme che definiscono i requisiti per la realizzazione, in un'organizzazione, di un sistema di gestione di qualità, al fine di condurre i processi aziendali, migliorare l'efficacia e l'efficienza nella realizzazione del prodotto e nell'erogazione del servizio, ottenere ed incrementare la soddisfazione del cliente;
- ISO 25000 SQuaRe, e successive, il modello di qualità del software e dei dati ed indicatori, linee guida per la relativa misurazione;
- Approcci metodologici di Project management che includono gli approcci agili, interattivi, incrementali e basati sulla successione di fasi predefinite (quali ad esempio: PMI, PRINCE2, IPMA COBIT, CMMI, ITIL, RUP, Agile, Devops, Togaf);
- Approccio metodologico per l'analisi, il disegno, la realizzazione e gestione di sistemi informatici complessi ed integrati;
- Metodologie specifiche e verticali del prodotto e/o piattaforma e/o soluzione tecnologica e/o pacchetto oggetto dell'intervento;
- Metodologie e strumenti per la stima ed il dimensionamento dei progetti software principalmente "FPA Function Point Analysis", "Early and Quick Function Point", "Simple Function Point", "Planning Poker", "WBS Estimation", "Three Point Estimation", ecc.
- Metodologie di testing quali ISTQB.

<u>Buone pratiche di collaborazione</u>

Il fornitore deve applicare metodologie di lavoro che seguano le buone pratiche di collaborazione e condivisione con l'Amministrazione Contraente, con gli altri operatori che hanno in carico la gestione operativa dei sistemi, altre aree applicative, ecosistemi, ecc, privilegiando metodologie agili e strumenti che massimizzino la chiarezza dei contenuti e degli obiettivi funzionali e non funzionali, e che riducano il rischio di incomprensioni e/o disallineamenti.