Capitolato Tecnico

Realizzazione dell'infrastruttura applicativa del Sistema Informativo Sanitario per la Regione Umbria

CIG derivato B0F58A02A6

Sommario

Sommario

Sommario

1. INTRODUZIONE

1.1 Finalità e struttura del documento

Il suddetto capitolato tecnico è volto a fornire descrizione dell'oggetto e dell'articolazione della fornitura richiesta dall'azienda PuntoZero s.c.a.r.l.; tale documento si propone, inoltre, di descrivere gli elementi fondamentali dell'offerta tecnica richiesta ai fini dell'aggiudicazione della procedura di acquisizione.

L'accordo che costituisce il punto di riferimento nello sviluppo della presente iniziativa è rappresentato dall'Accordo Quadro CONSIP "Servizi Applicativi in ambito "Sanità digitale - Sistemi informativi sanitari e servizi al cittadino" per le Pubbliche Amministrazioni del SSN sul Lotto applicativo N.4.

Gli elementi di carattere generale della presente iniziativa, quali, il contesto di riferimento, la strategia di approvvigionamento e le iniziative correlate sono discussi all'interno del Capitolo 2.

Nel Capitolo 3 è fornita la descrizione dell'oggetto della fornitura richiesta.

Nel Capitolo 4 e nel Capitolo 5 sono, invece, indicati i requisiti funzionali e i requisiti non funzionali, i quali sono fondamentali per definire il modello di riferimento sulla base del quale sarà sviluppata la proposta progettuale; all'interno del suddetto capitolo sono identificati, inoltre, le esigenze di supporto ai processi e i vincoli tecnologici.

In seguito, nel Capitolo 6, è identificata e descritta, in modo puntuale, nelle sue parti costitutive, l'architettura di riferimento della soluzione oggetto della fornitura, nonché il contesto della fase transitoria verso l'architettura di riferimento.

Il Capitolo 7 del presente documento, invece, è volto ad individuare i servizi professionali compresi nell'ambito della procedura di gara.

Nel Capitolo 8 sono riportate le specifiche inerenti ai servizi di realizzazione e delivery, gestione, assistenza, manutenzione della presente iniziativa; in modo particolare, si esplicitano le tempistiche previste per lo svolgimento delle attività, l'organizzazione complessiva delle stesse, gli strumenti previsti per favorire il coordinamento fra le Aziende Sanitarie e i rappresentati dei Fornitori e, si approfondiscono ulteriori servizi specialistici necessari.

Nel Capitolo 9 sono indicati i livelli di servizio, concernenti gli aspetti tecnici e gestionali del servizio che costituisce l'oggetto della fornitura; essi saranno, inoltre, oggetto di monitoraggio da parte delle Aziende Sanitarie durante l'esecuzione del contratto. I suddetti livelli di servizio costituiranno la base per la definizione dello schema delle penali contrattuali che saranno applicate in caso di inadempienza da parte delle Aziende Sanitarie.

Infine, nel Capitolo 10 è definita la gestione dei corrispettivi, mentre, nel Capitolo 11 sono indicati gli elementi dimensionali di riferimento del servizio.

Infine, il Capitolo 12 è interamente dedicato a tutti i processi, le attività e i requisiti necessari a garantire la sicurezza delle informazioni ed il mantenimento della privacy.

1.2 Glossario

Definizione	Significato	Descrizione
ADT	Accettazione, Dimissione, Trasferimento	Parte del Sistema Informativo che gestisce i processi (con relativa comunicazione) di accesso al ricovero, la movimentazione del paziente, la registrazione dell'esito del ricovero e la rendicontazione dei ricoveri.
ACO	Anagrafica Centrale Operatori	Soluzione per la gestione centralizzata delle anagrafiche degli operatori
AP	Anatomia Patologica	Soluzione a supporto delle attività di anatomia patologica
CCE	Cartella Clinica Elettronica	Un sistema informatico, ottimizzato per l'uso da parte del personale clinico e di assistenza, che durante un episodio clinico raccoglie i dati inerenti allo stato di salute e di cura individuale, attività ed eventi legati al paziente; supporta tutte le attività e integra dati provenienti da multiple fonti, interne ed esterne, ed i processi di diagnosi e di erogazione delle cure cliniche; supporta il processo decisionale degli operatori sulla base di sistemi di Knowledge Management clinico.
CDR	*Clinical Data Repository*	*Clinical data repository* aziendale di tutti gli eventi del paziente (referti, esami, ecc.) in formato sia documentale sia strutturato.
CUP	Centro Unico di Prenotazione	Sistema informativo dedicato al supporto dei processi di prenotazione ed erogazione nelle strutture dedicate alla gestione della domanda e dell'offerta di prestazioni specialistiche e di diagnostica.

Definizione	**Significato**	**Descrizione**
DTS	*Data Terminology server*	Sistema per la gestione delle codifiche e nomenclature.
FHIR	*Fast Healthcare Interoperability Resources*	È uno *standard* che descrive i formati e gli elementi dei dati, nonché un'interfaccia di programmazione dell'applicazione (API) per lo scambio di informazioni mediche. Lo *standard* è stato sviluppato da *Health Level Seven International* (HL7), un'organizzazione senza scopo di lucro dedicata allo sviluppo dell'interoperabilità dei dati sanitari e alla standardizzazione del protocollo di scambio medico.
Firma digitale		É un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.
FSE	Fascicolo Sanitario Elettronico	Si riferisce al Fascicolo Sanitario Elettronico regionale. É l'integrazione a livello regionale dei dati clinici generati dalle singole Aziende Sanitarie e registrati nei loro sistemi (*repository* dati clinici aziendali). Il cittadino e il personale sanitario autorizzato possono accedervi elettronicamente attraverso gli appositi servizi.
HL7	*Health Level Seven*	Standard XML per lo scambio di informazioni cliniche e amministrative.
I&PM	*Identity and Privacy Management*	Sistema atto a garantire un accesso controllato ai dati di tutte le applicazioni.

Definizione	Significato	Descrizione
KPI	*Key Performance Indicators*	Sono indicatori per la misurazione delle prestazioni valutando il successo di un'organizzazione o di una particolare attività (es. progetti). Forniscono un focus per il miglioramento strategico e operativo, creano una base analitica per il processo decisionale e aiutano a focalizzare l'attenzione su ciò che conta maggiormente.
LIS	*Laboratory Information System*	Sistema informativo per la gestione della diagnostica del Laboratorio di Analisi Chimico-Cliniche e Microbiologiche e dei relativi dati clinici.
MPI	*Master Patient Index*	Soluzione per la gestione centralizzata dell'anagrafica dei pazienti
OM	*Order Manager*	Modulo di *Order Entry* che gestisce le richieste di prestazioni sanitarie fornendo funzioni per la compilazione progressiva, gestione dello stato delle richieste e *monitoring*.
PACS	*Picture Archiving and Communication System*	Tecnologia per archiviare, recuperare, gestire, distribuire e presentare in modo sicuro immagini elettroniche
RIS	*Radiology Information System*	Soluzione a supporto del processo radiologico (prenotazione, accettazione, refertazione, firma digitale)
SLA (LdS)	*Service Level Agreement* (Livelli di Servizio)	Sono strumenti contrattuali attraverso i quali si definiscono le metriche di servizio (es. qualità di servizio) che devono essere rispettate da un fornitore di servizi (*provider*) nei confronti dei propri clienti/utenti. Di fatto, una volta stipulato il

Definizione	Significato	Descrizione
		contratto, assumono il significato di obblighi contrattuali.
SNOMED CT	*Systematized Nomenclature of Medicine - Clinical Terms*	Raccolta strutturata ed organizzata di terminologie mediche adottate nella maggior parte delle aree dell'informatica clinica (ad es. malattie, procedure, microorganismi, ecc.)
XML CDA2	*XML HL7 Clinical Document Architecture (CDA)* ver. 2	*Standard* basato su linguaggio XML finalizzato alla definizione delle modalità di codifica, strutturazione e semantica dei documenti clinici con l'obiettivo di facilitarne l'interscambio.

2. ELEMENTI GENERALI DELL'INIZIATIVA

2.1 Contesto di riferimento

La presente iniziativa si inscrive nel contesto di una pluralità di progetti intrapresi dalla Regione Umbria allo scopo di attuare le disposizioni prescritte dal Piano Nazionale di Ripresa e Resilienza, di seguito indicato come PNRR. Nell'ambito della missione 6 "Salute", il PNRR stabilisce due obiettivi primari **M6C1 e M6C2**.

In questo contesto, la missione di PuntoZero s.c.a.r.l. è rappresentata dall'obiettivo di tutelare e promuovere la salute dei cittadini, grazie a una rete integrata di servizi sanitari di prevenzione, cura e riabilitazione, oltre che servizi sociosanitari in ambito ospedaliero e domiciliare. PuntoZero si configura dunque come Ente di supporto al Sistema Socio-sanitario Regionale Umbro e, in particolare, alle quattro Aziende Sanitarie pubbliche del territorio: le Aziende Ospedaliere di Perugia e di Terni, l'USL Umbria 1 e l'USL Umbria 2, *di seguito aziende*, articolate nei diversi presidi come descritto nella tabella sottostante.

Azienda	Presidio	Tipo di presidio
Azienda Ospedaliera di Perugia	Perugia	Presidio DEA di II livello
Azienda Ospedaliera di Terni	Terni	Presidio DEA di II livello
USL Umbria 1	Assisi	
	Branca (Gubbio e Gualdo Tadino)	Presidio DEA di I livello
	Castiglione del Lago	
	Città della Pieve	Casa della Salute
	Città di Castello	Presidio DEA di I livello
	Media Valle del Tevere (Todi)	
	Passignano	Centro Ospedaliero di Riabilitazione Intensiva
	Poliambulatorio Europa (Perugia)	
	Umbertide	
	Capanne	Sanità penitenziaria
USL Umbria 2	Poliambulatori di Terni	

	Foligno	Presidio DEA di I livello
	Narni-Amelia	Ospedale di Comunità
	Orvieto	Presidio DEA di I livello
	Spoleto	Presidio DEA di I livello Sanità penitenziaria
	Norcia	Ospedale di Comunità
	Cascia	RSA

L'attuazione della **missione M6C1** prevede l'implementazione di una nuova strategia sanitaria che porti al conseguimento di standard di cura adeguati, allineati a quelli dei migliori paesi europei, e consideri il SSN parte di un più ampio sistema di welfare comunitario. Tale strategia prevede due filoni di attività principali:

- La definizione di ***standard* strutturali, organizzativi e tecnologici** omogenei per l'assistenza territoriale e l'identificazione delle strutture a essa deputate;
- La **definizione di un nuovo assetto istituzionale** per la prevenzione in ambito sanitario, ambientale e climatico, in linea con l'approccio *One-Health*.

In ambito organizzativo e tecnologico, **concorrono all'attuazione della nuova strategia diversi fattori,** tra i quali la creazione delle Case di Comunità e degli Ospedali di Comunità, la diffusione della telemedicina, il potenziamento dei servizi domiciliari e l'architettura per la raccolta e valorizzazione dei dati distribuiti, ovvero un modello architetturale basato su standard semantici per la raccolta, condivisione e utilizzo in tempo reale dei dati prodotti presso i diversi servizi sociosanitari di ambito ospedaliero e territoriale.

La **missione M6C2**, tramite l'investimento 1.1, si focalizza sull'**ammodernamento delle infrastrutture tecnologiche e digitali ospedaliere**. L'arretratezza in cui versano le infrastrutture di alcune Aziende Sanitarie incide negativamente sulla qualità delle prestazioni e dell'efficienza del sistema sanitario nazionale. L'investimento prevede l'ammodernamento digitale del parco tecnologico ospedaliero, tramite l'acquisto di nuove grandi apparecchiature ad alto contenuto tecnologico caratterizzate da una vetustà maggiore di 5 anni, sia con interventi finalizzati al **potenziamento del livello di digitalizzazione delle strutture sanitarie sede di Dipartimenti di emergenza e accettazione (DEA) di I e II livello**.

Nell'orizzonte dei possibili interventi di potenziamento del livello di digitalizzazione dei sistemi informativi ospedalieri regionali rientrano i seguenti:

- La creazione di un'**infrastruttura applicativa e servizi comuni** ai sistemi informativi sia a livello aziendale che a carattere regionale (Master Patient Index, Anagrafica centrale operatori, Clinical Data Repository, Identity and privacy management, Data Terminology server, middleware di integrazione locale)
- Progettazione e implementazione di un nuovo sistema per la gestione centralizzata dei **servizi di Laboratorio Analisi**;

- Progettazione e introduzione di un nuovo sistema gestionale centralizzato di **Anatomia Patologica*;***
- La creazione di un sistema centralizzato per la gestione dei **Servizi di Immunoematologia e Trasfusionale (SIT);**
- La creazione di un'unica struttura regionale capace di gestire in maniera centralizzata i dati del Sistema di gestione della Diagnostica per Immagini, attraverso l'evoluzione degli **attuali sistemi RIS e PACS, con l'introduzione di un VNA regionale centralizzato.**

L'infrastruttura applicativa risulta dunque essere rilevante per il conseguimento della missione M6C2, investimento 1.1. in quanto garantirà la costruzione delle fondamenta dei sistemi/a informativi per la sanità. Con questa gara si intende dotare le Aziende di un'infrastruttura di servizi comuni, attraverso componenti applicative unitarie, atta a garantire funzioni ed informazioni omogenee a supporto dei processi aziendali con l'obiettivo di perseguire il miglioramento continuo degli stessi.

La disponibilità di componenti unitarie a livello regionale, centralizzate in Cloud, apre rilevanti scenari di collaborazione tra i diversi attori sul territorio, in termini di condivisione delle informazioni, sempre in logica di privacy by design, e di interoperabilità tra i sistemi, nonché di scalabilità e adattività ai possibili mutamenti organizzativi e di processo.

Nell'esecuzione dei servizi oggetto del Presente Capitolato, il Fornitore dovrà altresì garantire il rispetto di tutti i requisiti tecnici e ambientali previsti dalla normativa europea e nazionale relativa al principio di non arrecare un danno significativo all'ambiente "*Do No Significant Harm*" (nel prosieguo, anche «**DNSH**»), ivi incluso l'impegno a consegnare all'Amministrazione la documentazione a comprova del rispetto dei suddetti requisiti.

In particolare, il Fornitore dovrà osservare tutti i requisiti relativi al principio DNSH previsti nei Regolamenti del Parlamento Europeo e del Consiglio n. 2020/852/UE del 18 giugno 2020 e n. 2021/2139/UE del 4 giugno 2021, negli *Operational Arrangements* del 22 dicembre 2021, nel CIS del 31 maggio 2022 e nei relativi allegati nonché, ove applicabili, nelle schede tecniche contenute nella «*Guida operativa per il rispetto del principio di non arrecare danno significativo all'ambiente (cd. DNSH)*» di cui alle circolari del Ministero dell'Economia e delle Finanze, Dipartimento della Ragioneria Generale dello Stato n. 32 del 30 dicembre 2021 e n. 33 del 13 ottobre 2022 e negli eventuali ulteriori atti di programmazione relativi al presente intervento.

2.2 Obiettivi dell'iniziativa

La presente iniziativa traduce operativamente quanto definito a livello strategico nel **Programma Attuativo dell'Ecosistema di servizi di sanità digitale 2023-2026** (di seguito "Programma"), definito in raccordo con Il "Master-plan della Regione Umbria per la semplificazione e l'agenda digitale 2023-2025" (d'ora in poi Master-plan).

Il suddetto Programma definisce l'**architettura di alto livello dell'Ecosistema per i servizi di sanità digitale,**

realizzata con l'obiettivo di consolidare gli investimenti sostenuti nel passato, favorendo una logica di evoluzione e upgrade tecnologico, ma anche sfruttare sinergie organizzative e tecniche, nonché economiche, che deriveranno da un'architettura che centralizza alcuni dei servizi strategici, come appunto la componente di infrastruttura applicativa e altri applicativi (es. RIS/PACS, VNA, SIT, LIS, Anatomia patologica).

L'obiettivo è di dotare il Sistema Sanitario della Regione Umbria di servizi comuni a supporto degli applicativi a carattere regionale (es. RIS/PACS e VNA, SIT, LIS, Anatomia patologica) e quelli verticali presenti per le diverse aziende (es. CCE, ADT ecc.). La realizzazione di componenti unitarie a livello regionale rappresenta un elemento strategico e imprescindibile per il raggiungimento degli obiettivi di potenziamento della digitalizzazione posti dal PNRR, per incrementare il patrimonio informativo regionale di ambito sanitario e per implementare i nuovi scenari di integrazione tra i servizi ospedalieri e territoriali, anche in ragione del conseguimento degli obiettivi delineati nel PNRR, in cui il modello EMRAM funge da strumento di valutazione dell'efficacia globale delle iniziative destinate ai DEA di primo e secondo livello. In linea con l'insieme delle altre iniziative regionali pianificate, la realizzazione dei servizi comuni consentirà di soddisfare appunto i requisiti minimi richiesti dal Modello EMRAM (HIMSS).

Gli obiettivi principali dell'iniziativa sono i seguenti:

- Attuare progressivamente una nuova infrastruttura applicativa a carattere regionale per i sistemi informativi, superando l'attuale frammentazione, promuovendo l'interoperabilità e l'ottimizzazione dell'uso dei dati nell'intera Regione.
- Favorire l'ottimizzazione dei processi di ambito ospedaliero e territoriale attraverso l'implementazione di nuovi scenari di interoperabilità applicativa con condivisione di dati in tempo reale e in modalità controllata e sicura.
- Abilitare lo scambio strutturato di dati tra le diverse organizzazioni in diversi contesti.
- Abilitare e promuovere l'analisi strutturata dei dati raccolti durante i percorsi di cura dei pazienti con utilizzo delle informazioni a livello locale e regionale, sempre nel rispetto della privacy.
- Consentire la crescita dei volumi dei dati, delle transazioni e del portafoglio di servizi applicativi erogati grazie a componenti unitarie scalabili.
- Favorire una forte integrazione e coerenza tra le componenti applicative comuni e orientamento agli standard.

2.3 Iniziative correlate

La progettualità di cui all'oggetto della presente fornitura rappresenta le fondamenta per il funzionamento di un sistema informativo sanitario evoluto; pertanto, impatta su molte delle iniziative in corso di realizzazione, nonché sui sistemi in esercizio.

Nello specifico, la realizzazione dell'investimento **M6C2 I1.1.1 Ammodernamento del parco tecnologico e digitale ospedaliero - Digitalizzazione (DEA di I e II livello)** si compone, oltre alla progettualità in oggetto, di una serie di iniziative strategiche che rappresentano un tassello importante per il futuro delle sanità dell'Umbria.

- Realizzazione di nuovo sistema per la gestione centralizzata dei **servizi di Laboratorio Analisi (LIS)**;
- Realizzazione di un sistema gestionale centralizzato di **Anatomia Patologica (AP)*;***
- Realizzazione di un sistema centralizzato per la gestione dei **Servizi di Immunoematologia e Trasfusionale (SIT);**
- Realizzazione di un'unica struttura regionale capace di gestire in maniera centralizzata i dati del Sistema di gestione della Diagnostica per Immagini, attraverso l'evoluzione degli **attuali sistemi RIS e PACS, con l'introduzione di un VNA regionale centralizzato;**

Inoltre, in relazione all'investimento **1.3.1 Rafforzamento dell'infrastruttura tecnologica e degli strumenti per la raccolta, l'elaborazione, l'analisi dei dati e la simulazione (FSE) - (M6C2 I1.3.1), la** Regione Umbria è chiamata a realizzare una serie di interventi previsti nel Piano di Adeguamento Tecnologico (PAT) del Fascicolo Sanitario Elettronico, verso FSE2.0.

2.4 Estensione complessiva e intervallo temporale dell'iniziativa

Al progetto aderiscono, con le modalità descritte nei capitoli successivi, le quattro Aziende (USL e AO) della Regione Umbria che hanno manifestato l'intenzione di evolvere l'architettura dei sistemi attraverso la realizzazione di un'infrastruttura applicativa (servizi comuni) centralizzata.

Le previsioni relative alla durata del progetto includono un **periodo totale di 48 mesi**, inizianti dalla firma del Contratto Esecutivo, con la seguente suddivisione:

- Entro il 3° mese dalla stipula del contratto: analisi del Sistema Informativo di ciascuna Azienda Sanitaria e formalizzazione di un **Piano Esecutivo di Progetto** (da concordare con le Aziende Sanitarie, il Fornitore aggiudicatario e Regione Umbria e PuntoZero) che contempli la declinazione delle tempistiche complessive, dettagli operativamente gli obiettivi di risultato e le modalità realizzazione della transizione per le implementazioni nelle organizzazioni interessate, i meccanismi di coordinamento tra Regione/PuntoZero s.c.a.r.l., il Fornitore aggiudicatario, le Direzioni delle Aziende Sanitarie/Ospedaliere delineati in sede di gara. Infine, *il Fornitore aggiudicatario sarà vincolato alla interazione, anche diretta, con i fornitori degli applicativi in uso che dovranno integrarsi e con gli applicativi oggetto delle iniziative correlate e descritte nel presente capitolato (rif.2.3), nonché con i fornitori degli applicativi che dovranno interfacciarsi con gli oggetti della fornitura;*
- Entro il 5° mese dalla stipula del contratto: formalizzazione del **Piano Operativo di progetto** di introduzione e diffusione sulla singola Azienda che contempli, mediante GANTT, la declinazione delle tempistiche e che dettagli operativamente gli obiettivi e il piano di introduzione e diffusione sulle singole organizzazioni coinvolte;
- Entro il 12°-13° mese dalla stipula del contratto (non oltre giugno 2025): **realizzazione e collaudo delle soluzioni oggetto di fornitura per tutte le quattro Aziende;**
- A partire dal collaudo, messa in esercizio, supportando le Aziende nella fase di transizione al nuovo sistema, formazione e completamento della diffusione in ciascuna Aziende sanitaria, nonché **gestione a regime della soluzione** fino a fine contratto.

Sulla base di quanto sopra indicato, si richiede al Fornitore aggiudicatario che i **sistemi siano collaudati per tutte e quattro le Aziende** aderenti **entro giugno 2025**, **al fine di rispettare le milestone PNRR**.

Si allega al presente documento un'ipotesi di programmazione GANTT (allegato "AS_Infrastruttura applicativa ipotesi macro gantt"), che potrà essere migliorata in sede di presentazione di offerta tecnica.

2.5 Modello di approvvigionamento

PuntoZero s.c.a.r.l., a seguito dell'incarico assegnatole da parte di Regione Umbria, ha raccolto le deleghe da ciascuna Azienda sanitaria aderente all'iniziativa e, sulla base dei fabbisogni espressi dagli stessi, ha elaborato quanto utile all'esperimento del presente appalto specifico.

Ciascuna Azienda sanitaria aderente stipulerà con il fornitore identificato un **contratto esecutivo aziendale diretto della durata di 48 mesi** valorizzato sulla base delle esigenze specifiche della singola Azienda Sanitaria. La valorizzazione del singolo contratto esecutivo e delle specifiche componenti di servizio deriverà dall'applicazione degli sconti offerti dal fornitore agli elementi economici dettagliati nel presente Capitolato.

3. OGGETTO DELLA FORNITURA

La fornitura prevede la provvisione dei servizi professionali e degli elementi software necessari per la realizzazione e diffusione di una soluzione di infrastruttura applicativa avanzata per il sistema sanitario regionale.

Nel seguito vengono presentate le componenti applicative oggetto della fornitura, mentre nel capitolo 4, vengono presentati i relativi requisiti funzionali:

- **Anagrafiche centralizzate - Master Patient Index (MPI)**: un'anagrafica principale dei pazienti (MPI) a livello regionale, gestita in modo centralizzato.
- **Anagrafica Centrale Operatori (ACO):** un'anagrafica degli operatori centralizzata a livello regionale, alimentata dalle anagrafiche del personale gestite con il sistema di gestione del personale Sigma, in cui vanno introdotte anche figure non dipendenti (es. praticanti, specializzandi, medici a gettone, etc.).
- **Clinical Data Repository (CDR):** un Clinical Data Repository centralizzato a livello regionale per favorire:
  - Orientamento al paziente: gestire in maniera integrata l'informazione clinico-sanitaria;
  - Orientamento ai processi: supportare gli operatori nella gestione dei percorsi e, in prospettiva, alla ricerca;
  - Dematerializzazione dei processi e dei dati clinici: il trattamento delle informazioni deve essere conforme alle normative vigenti (firma digitale e privacy);
  - Modularità e Scalabilità della soluzione: per consentire la crescita dei volumi dei dati, delle transazioni e del portafoglio di servizi applicativi erogati;

- Flessibilità, Personalizzabilità e Adattività per consentire un facile adeguamento ai possibili mutamenti organizzativi e di processo, nonché alle diverse esigenze delle unità operative aziendali;
- Forte integrazione e coerenza tra le componenti della soluzione e orientamento agli standard;
- Facilità d'utilizzo attraverso l'adozione di semplici interfacce utente di facile apprendimento ed un disegno snello delle transazioni applicative.

Il CDR deve favorire la condivisione dei dati tra gli attori (ospedale e territorio), tramite accessi controllati, e permettere di integrare e standardizzare, in modo principalmente strutturato ma anche non strutturato, le informazioni.

Dal CDR dovrà essere possibile integrarsi con il gateway nazionale, attraverso il middleware regionale, per la validazione dei documenti e la successiva pubblicazione su FSE2.0. Il middleware regionale esporrà, per tutti i servizi implementati dal gateway nazionale, le stesse API oltre ad ulteriori API per i servizi di ricerca e recupero documento.

- **Identity & privacy management (I&PM):** l'Identity Privacy Management è essenziale per garantire un accesso controllato ai dati clinici dei pazienti al CDR in base alle scelte di privacy e consensi rilasciati dagli stessi. In prospettiva, permettere l'accesso controllato, basandosi sui ruoli e i permessi degli utenti, ai dati clinici dei pazienti da parte di qualsiasi applicativo del SIO.
- **Data Terminology Server (DTS):** un DTS per centralizzare la gestione applicativa delle codifiche, garantendo l'interoperabilità semantica, che permette di definire standard di codifica e terminologia comuni che possono essere utilizzati da diversi applicativi o sistemi all'interno di un'organizzazione sanitaria, anche quando usati riferimenti terminologici diversi all'interno degli applicativi.
- **Middleware di integrazione locale:** middleware d'interoperabilità locale in modo da consentire l'interscambio da e verso le applicazioni di ASL e AO. **E' oggetto della presente fornitura solo il middleware locale per la USL 2 e Azienda Ospedaliera di Terni**. Il middleware locale dovrà garantire la continuità operativa e interfacciarsi con il middleware regionale (digital integration hub) già presente.

L'**oggetto della fornitura deve comprendere le licenze d'uso** per tutte le componenti software, nessuna esclusa, richieste nel presente Capitolato. Come stabilito dalla direttiva del 19 Dicembre 2003, ove possibile, **le componenti devono basarsi su tecnologie open o, in alternativa, vanno garantite le licenze d'uso proprietarie fornite a tempo illimitato (perpetuo) e con titolarità a favore dell'ente appaltatore**.

Il nuovo sistema di infrastruttura applicativa deve essere implementato come soluzione unica regionale, centralizzata in cloud presso Cloud PA idoneo, secondo le caratteristiche di compatibilità di cui al paragrafo 6.4 "Infrastruttura tecnologica", e integrata con i sistemi informativi delle Aziende Sanitarie e Ospedaliere aderenti attraverso i servizi di interoperabilità messi a disposizione dal *Digital Integration Hub regionale e middleware di integrazione* aziendali.

La fornitura, oltre alle tecnologie e servizi professionali per l'implementazione della nuova soluzione applicativa, deve comprendere anche i seguenti servizi per tutta la durata del contratto:

- Realizzazione della soluzione di infrastruttura applicativa, che include analisi, installazione, configurazione ed integrazioni, in tutte le sue componenti;
- Creazione e messa a disposizione di un ambiente di test da utilizzare prima di ottenere il rilascio in produzione e, in seguito, per ogni manutenzione evolutiva;
- Collaudo, messa in esercizio della nuova soluzione e diffusione della soluzione nel suo complesso;
- Formazione al personale utilizzatore dei sistemi e servizi ICT;
- Manutenzione Adeguativa e manutenzione Correttiva della nuova soluzione nel suo complesso;
- Conduzione tecnica compresa la gestione di tutte le componenti applicative (ad esempio Database) al fine di mantenere i sistemi sempre attivi e funzionanti
- Conduzione tecnica per quanto riguarda il supporto infrastrutturale per la presa in carico e messa in esercizio delle infrastrutture HW nonché l'attività di Help Desk di 2 livello finalizzata alla risoluzione delle problematiche legate all'utilizzo delle infrastrutture in conduzione.
- Assistenza (help desk);
- Adeguamento normativo regionale e nazionale per l'intero periodo contrattuale.

Sono parte integrante della Fornitura tutte le attività di project management necessarie alla realizzazione ed erogazione delle componenti principali della soluzione. Le caratteristiche degli elementi di Fornitura sono dettagliatamente descritte nei Capitoli successivi.

4. REQUISITI FUNZIONALI

Nel presente capitolo si riportano i requisiti funzionali minimi che sono richiesti nel presente Capitolato rispetto ai quali il Fornitore può formulare un'offerta esclusivamente maggiorativa dal punto di vista funzionale.

4.1 Master Patient Index (MPI)

Si riportano nel seguito i requisiti funzionali relativi all'MPI:

- deve integrarsi come slave con l'Anagrafe Regionale Assistiti (ARA), sistema master e gateway, per reperire i dati anagrafici degli assistiti/assistibili gestiti su ARA. Le integrazioni dovranno avvenire utilizzando API REST, API FHIR o messaggi HL7 v.2.5; le modalità di integrazione per i diversi flussi verranno indicate da PuntoZero;
- deve consentire il tracciamento, integrandosi con l'Anagrafe Sanitaria Regionale, di tutti gli eventi significativi socio-sanitari del cittadino, come ad esempio: decesso, immigrazione/emigrazione (passaggio di assistenza da una ad altra azienda sanitaria), scelta/revoca del medico di base, rilascio delle esenzioni al pagamento ticket, sospensione assistenza sanitaria, esenzioni attualmente attive, disattivazione esenzioni con data fine con visibilità dello storico dei dati modificati etc.;
- deve allinearsi con ARA in modalità sincrona;
- deve integrarsi con l'Anagrafica Nazionale Assistiti (ANA) per reperire i dati di assistiti non regionali per mezzo dei servizi esposti da ARA (che sarà utilizzato come gateway) ed implementare i servizi

per il recupero e la verifica delle anagrafiche tramite codice fiscale e/o altri dati anagrafici (es. nome, cognome, data di nascita ecc);

- deve consentire l'inserimento di un nuovo assistito in anagrafica;
- deve consentire l'identificazione univoca di un cittadino nell'ambito di tutti gli episodi di cura e nelle diverse fasi in cui vengono erogate prestazioni gestite dal sistema informativo aziendale mediante:
    - lettura dalla tessera sanitaria regionale o nazionale o del Codice Fiscale del paziente;
    - digitazione di un set, anche parziale, dei suoi dati anagrafici.
- deve gestire tutti i codici/casi d'uso (STP-Straniero Temporaneamente Presente, ENI, TEAM, PASSAPORTO etc). La procedura di gestione dovrà aderire alla normativa vigente a livello nazionale e regionale;
- deve consentire la consultazione dello storico degli inserimenti/modifiche anagrafiche, la verifica delle cause di non validità del record e dello stato degli allineamenti con l'anagrafica regionale effettuate in back office;
- deve consentire l'allineamento in tempo reale tra l'anagrafe a livello dipartimentale e quella centrale a seguito di modifica o inserimento locale secondo opportune regole e permessi;
- deve consentire la gestione delle richieste di anonimizzazione del paziente in uno specifico evento di contatto;
- deve essere integrabile con il modulo di profilazione degli operatori (IPM) che vi accedono con possibilità di configurare ruoli e relativi permessi per la visualizzazione e modifica dei dati e la generazione dei report;
- deve consentire la storicizzazione delle modifiche operate a ogni titolo ai record anagrafici con tutti i dati di corredo: utente, date e ora, modifica effettuata, etc.;
- deve consentire la consultazione, inserimento, modifica, unificazione e la validazione di posizioni anagrafiche in maniera manuale ed attraverso elaborazioni automatiche massive;
- deve consentire la configurazione di regole per la validazione dei dati secondo specifiche politiche e per la correzione di problematiche legate ad esempio alle duplicazioni;
- deve consentire l'esecuzione di estrazioni massive e/o filtrate di posizioni anagrafiche duplicate e di attivazione temporalmente programmata delle relative unificazioni (confluenze anagrafiche);
- deve consentire la visualizzazione, con opportuni e molteplici filtri selettivi, degli inserimenti, modifiche e/o unificazioni eseguite e degli esiti dei relativi controlli con specificazione dell'origine della movimentazione;
- il record anagrafico deve contenere le informazioni del tipo di certificazione/validazione per i dati anagrafici del paziente e deve consentirne la modifica (manuale e automatica) in base al livello di certificazione (MEF, NAR e locale etc.). Deve inoltre importare, in maniera automatica, sul record di più alto livello eventuali informazioni mancanti che risultano disponibili sui record di livello inferiore;
- il record anagrafico deve contenere le informazioni relative alla lingua del paziente ed alla nazione di provenienza;
- deve gestire la trasmissione delle variazioni anagrafiche verso sistemi terzi per gli opportuni allineamenti (modalità "PUSH").

4.2. Anagrafe Centrale degli Operatori (ACO)

Si riportano nel seguito i requisiti funzionali relativi all'ACO:

- deve gestire secondo una logica centralizzata, le regole di accesso degli operatori sui diversi applicativi delle diverse aziende ospedaliere e ASL, ad esempio: FSE, CDR, SAR, CUP, sistemi di diagnostica e dipartimentale (es. LIS, RIS/PACS, AP, SIT), sistemi verticali (es: CCE, ADT), sistemi territoriali, Sistema TS (per i medici prescrittori inclusi MMG e PLS);
- deve consentire l'associazione dinamica dell'operatore con data inizio e fine validità ad un opportuno profilo professionale (medico, infermiere OSS, ostetrico, anestesista, etc.) - dipendente e non dipendenti;
- deve consentire l'associazione dinamica dell'operatore con data inizio e fine validità alla struttura organizzativa di appartenenza (struttura, reparto, ambulatorio, ufficio centrale, etc.) e i relativi centri di costo;
- deve consentire di consultare lo storico degli inserimenti/modifiche anagrafiche, verificare le cause di eventuale non validità del record;
- deve consentire l'inserimento, modifica o eliminazione di un nuovo operatore in anagrafica:
    - l'identificazione univoca di un nuovo utente;
    - la storicizzazione delle modifiche operate;
    - l'autenticazione univoca dell'utente mediante certificato, scheda elettronica, nome utente e password o altro supporto;
    - la consultazione, l'inserimento, la modifica e l'unificazione di singole posizioni anagrafiche;
    - la visualizzazione, con opportuni e molteplici filtri selettivi, degli inserimenti, modifiche e/o unificazioni eseguite e degli esiti dei relativi controlli con specificazione dell'origine della movimentazione;
- deve consentire l'identificazione univoca di un nuovo utente;
- deve consentire la storicizzazione delle modifiche operate;
- deve consentire l'autenticazione univoca dell'utente mediante certificato, scheda elettronica, nome utente e password o altro supporto;
- deve consentire la consultazione, l'inserimento, la modifica e l'unificazione di singole posizioni anagrafiche;
- deve consentire la visualizzazione, con opportuni e molteplici filtri selettivi, degli inserimenti, modifiche e/o unificazioni eseguite e degli esiti dei relativi controlli con specificazione dell'origine della movimentazione;
- deve consentire la configurazione di regole automatiche per la validazione dei dati secondo specifiche e per la correzione di problematiche legate ad esempio alle duplicazioni;
- deve consentire l'attivazione dell'allineamento anagrafico con i sistemi che ne fanno uso in modo sincronizzato o on demand;
- deve consentire l'esecuzione di estrazioni di massa, ma selettive di posizioni anagrafiche duplicate e di attivazione temporalmente programmata delle relative unificazioni.

4.3. Clinical Data Repository (CDR)

Si riportano nel seguito i requisiti funzionali relativi al CDR

- deve gestire tutto il ciclo di vita del dato: acquisizione nei diversi formati; gestione del dato intesa come controllo, indicizzazione e verifica dell'integrità delle informazioni acquisite; firma secondo gli standard di riferimento; conservazione e archiviazione del dato;
- deve supportare lo standard CDA2 non solo a livello di memorizzazione, ma anche per la visualizzazione dei documenti, per la ricerca all'interno dei tag XML, e per la rappresentazione grafica dell'andamento dei dati nel tempo;
- deve gestire documenti nei seguenti formati: HL7 CDA R2 con e senza firma, PDF, P7M e M7M, RTF, XML;
- deve comprendere un server FHIR che metta a disposizione le risorse in formato HL7 FHIR corrispondenti ai dati gestiti nel CDR;
- i dati registrati nel CDR in formato CDA2 possono essere mappati in risorse FHIR in modo da poterne usufruire in una logica di FHIR server;
- per l'alimentazione da altri applicativi, oltre alla conformità alle transazioni in standard XDS.b, è necessario che siano supportati i messaggi HL7 di tipo MDM contenenti un pdf in formato CDA2 in modo da registrarli come se fossero delle transazioni XDS.b di tipo ITI-41 (tramite un modulo specifico o attraverso la customizzazione di appositi canali di trasformazione su ESB);
- è necessario supporti la registrazione di Dicom Manifest per garantire la corretta correlazione tra referti ed immagini diagnostiche registrate nel VNA;
- la soluzione gestisce la visualizzazione delle immagini in formato DICOM mediante integrazione con viewer esterno del VNA;
- la soluzione è in grado di gestire e archiviare i Manifest DICOM KOS prodotti dai sistemi PACS contenenti i riferimenti alle istanze DICOM;
- è certificato IHE (certificazione disponibile nei connect-a-thon results) per le transazioni di tipo XDS.b e XDS-I.b, MHD, MPQ, RMD, QEDm, CT, ATNA e DSUB di IHE;
- supporta i profili Provide and Register Document Set (popolamento repository), Register Document Set (popolamento register), Retrieve Document Set (recupero documento dal repository);
- per l'implementazione della specifica HL7 FHIR per Java, la soluzione è in grado di supportare la libreria HAPI FHIR versioni DSTU3 o R3 e R4 (anche possibilmente R5);
- viene gestito il collegamento logico tra documenti/informazioni strutturate per episodio/contatto e correlate con altre informazioni es. data e ora registrazione, e autore registrazione;
- la soluzione gestisce la storicizzazione e il versioning dei dataset, assicurando l'integrità e la coerenza del CDR;
- la soluzione è in grado di tracciare tutti gli accessi alle informazioni e ai documenti, ed è presente un'interfaccia web based e dei servizi web REST per la consultazione degli accessi;
- per le modalità della comunicazione da front-end al back-end deve essere disponibile la crittografia a livello di applicazione (tra client e web server);

- l'accesso da remoto ai sistemi avviene tramite protocolli crittografici (TLS / SSL) in grado di garantire la riservatezza e l'integrità delle informazioni trasmesse tra il client remoto e il sistema interno;
- le operazioni di attività degli utenti sono tracciate su sistema di AUDIT con persistenza su DB. Si richiede inoltre la compliance con il profilo d'integrazione ATNA (Audit Trail and Node Authentication);
- deve permettere l'accesso in forma strutturata alle fasi precedenti del percorso di cura del paziente e consentire l'importazione di parte o tutto il contenuto presente nei referti stilati negli episodi clinici precedenti dello stesso ambulatorio o reparto o unità di pre-ricovero, nei rispettivi campi tematici previa esplicita autorizzazione del clinico prima dell'importazione;
- la consultazione degli episodi/referti del singolo paziente depositati CDR tramite funzionalità di navigazione che permettano:
    - *la filtrabilità degli episodi per data, tipo prestazione, tipo episodio, diagnosi codificata, problema attivo;*
    - *l'accesso allo storico degli episodi anche tramite funzionalità di visualizzazione in forma grafica (cronistoria o Albero degli Eventi);*
    - *la consultazione dei documenti sia in forma strutturata (ove disponibile) sia in forma di referto pdf firmato digitalmente;*
- la navigazione tra la totalità dei dati e documenti del CDR deve permettere di:
    - *filtrare gli episodi per data, tipo prestazione, tipo episodio, diagnosi codificata, problema attivo;*
    - *accedere allo storico degli episodi tramite funzionalità della CCE di visualizzazione in forma grafica (cronistoria o Albero degli Eventi);*
    - *la consultazione dei documenti sia in forma strutturata sia in forma di referto pdf firmato digitalmente;*
- deve essere multilingue e supportare, al minimo, la lingua italiana;
- deve essere web based responsive e compliant con specifiche HTML5;
- deve prevedere la crittografia del DB per finalità di sicurezza con strumenti trasparenti per le applicazioni;
- deve avere già preimpostati i Dataset di informazioni strutturate da gestire previsti dal FSE 2.0 (anatomia patologica, vaccinazioni, etc.);
- fornire strumenti per la modifica o definizione dei dataset con interfacce user friendly che non prevedano l'intervento di tecnici che "programmino" le modifiche;
- possibilità di autocertificazione (con obbligo di motivazione) per accedere ai dati di un paziente in caso di emergenza (solo per i documenti non oscurati).

4.4. Identity e Privacy Management (I&PM):

Si riportano nel seguito i requisiti funzionali relativi all'I&PM

- deve registrare in maniera del tutto centralizzata, ossia in un unico punto, i consensi del paziente rispetto al trattamento dei propri dati personali affinché la gestione degli stessi sia aderenti alla vigente normativa GDPR 679/2016;
- modulare l'accesso ai dati clinici, super sensibili, dello stesso cittadino da parte del personale impiegato in funzione del tipo di consenso prestato all'atto della registrazione;
- mettere a disposizione dello stesso personale uno spazio unico in cui tutte le soluzioni software di terze parti già in uso presso le aziende (AO/USL), a seconda del proprio utilizzo, potranno inviare il consenso eventualmente raccolto;
- necessità di garantire una corretta gestione tanto dei consensi informati alla prestazione sanitaria quanto dei consensi al trattamento dei dati personali dell'interessato per specifiche finalità di trattamento;
- garantire una configurazione coerente con la normativa di riferimento e si dovrà interfacciare con il CDR, affinché siano attuate le azioni consequenziali alle decisioni indicate dai pazienti in termini di trattamento dei dati (comunicazione, consultazione, conservazione);
- oltre alla regolazione del sistema degli accessi, deve essere prevista la crittografia (es. omomorfica), il partizionamento dei dati, un sistema di alert che evidenzi eventuali accessi ripetuti sui dati del paziente da parte di personale autorizzato (sistema di AUDIT);
- deve gestire la revoca del consenso da parte del cittadino;
- deve rispettare i criteri e le autorizzazioni in merito alla consultazione dei dati clinici compresi gli eventuali oscuramenti e oscuramenti degli oscuramenti restituendo tali regole tramite web services agli applicativi che ne faranno richiesta per autorizzare correttamente l'accesso da parte del personale clinico ai dati clinici del paziente;
- deve gestire il consenso per pazienti minori e di adulti con incapacità di intendere e volere;
- deve supportare il protocollo IHE BPPC (Basic Patient Privacy Consents);
- deve prevedere la possibilità di crittografare il DB;
- deve prevedere la possibilità di autorizzare l'accesso ai dati in base a diversi livelli logici (es. accesso ai dati obbligatori FSE, accesso selettivo ai dati opzionali FSE, nessun accesso ai dati clinici per uso interno della struttura).

4.5. Data Terminology Server (DTS)

Si riportano nel seguito i requisiti funzionali relativi al DTS:

- deve consentire una gestione centralizzata delle codifiche aziendali e governare le banche dati condivise tra le varie applicazioni a livello delle aziende al fine di favorire la costituzione di un modello dati unico integrato;
- deve consentire la standardizzazione delle codifiche dei codici ISTAT, comuni (es. esteri) che devono essere allineati con quelli in uso da ANA e ANPR;
- i dati che esprimono i valori dei nomenclatori delle codifiche possono ad un livello avere un'espressione diversa rispetto agli omologhi dati espressi ad un livello diverso, di conseguenza è supportata una transcodifica (mapping) che definisca le corrispondenze fra i diversi formalismi;

- deve essere multilingue e supportare, al minimo, la lingua italiana;
- deve includere un nomenclatore delle prestazioni e il tariffario;
  - catalogo prestazioni regionale;
  - tabella di codifica degli attributi possibili per le prestazioni (es. metodiche, lateralità, etc.);
  - codici dei DRG (Diagnosis Related Groups) con i relativi importi;
  - codifiche dei vari tipi di prestazioni (es: visita 626, visita domiciliare, etc.);
  - tabella di codifica dei tipi di assistenza ministeriali (es. Assistenza domiciliare, SASN, etc.);
  - tabella di codifica delle modalità di erogazione delle prestazioni (es. Ordinario, Pronto Soccorso, etc.);
- deve includere le classi di codifiche cliniche – sanitarie (es. Tabella Codici degli MDC (Major Diagnostic Categories);
- deve includere le classi di codifiche amministrative;
- lo strumento deve essere in grado di supportare, oltre ai principali standard internazionali di riferimento per le codifiche clinico sanitarie (SNOMED CT, LOINC, CPT, RxNorm, ICD-9-CM, ICD-10-CM, LOINC, CPT, HCPCS, DSM-IV-TR, etc...), le sottoclassi di codifiche aziendali presenti. Lo strumento deve inoltre essere aggiornabile nel tempo nel caso si renda necessaria la gestione di ulteriori classi e sottoclassi di codifiche;
- deve prevedere la gestione di tutte le tabelle di dominio e la loro esposizione in forma di servizio a tutti gli applicativi locali interessati, con opportuni meccanismi di distribuzione e aggiornamento a tutti i livelli. Questa parte dovrà occuparsi anche della gestione delle transcodifiche e fornire gli strumenti di traduzione tra le codifiche centrali e le codifiche dei singoli applicativi facenti parte del Sistema Informativo;
- deve consentire l'inserimento, la modifica o l'eliminazione logica di un record;
- deve consentire l'identificazione univoca delle prestazioni richieste nell'ambito di tutti gli episodi di cura e nelle diverse fasi in cui vengono erogate prestazioni gestite dal sistema informativo;
- deve consentire la condivisione delle informazioni con le varie applicazioni facenti parte del sistema informativo. Le informazioni dovranno essere rese disponibili attraverso lo strato di integrazione secondo modalità standard (web services) al fine di alimentare sistemi terzi quali, ad esempio, database scientifici o sistemi di tracciabilità;
- deve consentire la transcodifica delle informazioni scambiate con sistemi dipartimentali e con i sistemi nazionali e viceversa;
- deve fornire la possibilità di aggiornare le codifiche su applicativi esterni a fronte di aggiornamenti delle codifiche interne.

Rispetto alla **realizzazione del DTS saranno da considerare i due possibili scenari**:

- Scenario 1: disponibilità del Terminology system (terminology server FHIR basato su HAPI), e specifiche tecniche, a livello nazionale. Si richiedere al Fornitore di analizzare le specifiche funzionali del codice open source del terminology nazionale, rispettando i requisiti funzionali indicati nel presente capitolato, e di dare evidenza della fattibilità tecnica di uso del codice open per il contesto

regionale umbro in sede di presentazione dell'offerta, azzerando quindi il costo delle licenze di prodotto (come previsto anche al paragrafo 5.7);

- Scenario 2: non disponibilità del Terminology system nazionale nei tempi utili di sviluppo dell'oggetto della fornitura; si richiede al Fornitore di prevedere modalità di allineamento del DTS regionale con quello nazionale per evitare che dizionari regionali non censiti a livello nazionale possano condizionare una corretta gestione comune delle terminologie.

4.6. Middleware locale per USL 2 e Azienda Ospedaliera Terni

Si riportano nel seguito i requisiti funzionali relativi al middleware locale

- deve garantire elevate performance e scalabilità;
- deve essere configurato in alta affidabilità;
- deve essere multipiattaforma rispetto all'hardware e al sistema operativo (Windows, Linux, etc)
- deve supportare la gestione publish / subscribe ed event driven;
- deve garantire le attività di routing basandosi sia sugli standard internazionali di instradamento (ws: addressing e simili) che sul contenuto dei messaggi;
- deve offrire i servizi di test per validare le diverse componenti delle interfacce;
- deve fornire la persistenza di tutti i messaggi e dei processi attraverso la presenza di un RDBMS quale parte integrante dell'offerta;
- deve gestire un motore di regole (Business Rules Engine, BRE) estensibile ed utilizzabile in modo efficace anche da non programmatori;
- deve garantire il log e la tracciabilità di tutte le operazioni e messaggi gestiti; in particolare deve avere un'interfaccia grafica per il log, il monitoraggio la tracciabilità dei messaggi (Business Activity Monitoring, BAM), il loro recupero, la loro visualizzazione, l'eventuale modifica e re-inoltro nel processo, sia in fase di sviluppo (per operazioni di debug), sia in produzione; deve essere inoltre possibile monitorare i livelli di servizio (Service Level Monitoring, SLM) e gli indicatori chiave di performance per ogni servizio/metodo esposto/proxato anche attraverso cruscotti grafici integrati;
- deve avere un motore per la gestione di Business Process (Business Process Management, BPM)
- deve essere gestito il versioning per i servizi ed i processi resi disponibili attraverso l'ESB;
- deve garantire che i messaggi vengano processati ed instradati nella sequenza stabilita dal mittente (sequencing);
- deve supportare i formati di messaggistica standard in sanità, tra cui HL7, DICOM, ASTM, CDA2, FHIR;
- la messaggistica HL7 oltre ad essere integrata con tutte le altre funzionalità e caratteristiche esposte, deve garantire la documentazione ed il supporto nativo per le versioni 2.X e 3;
- deve supportare i profili IHE per gestire gli scenari di interoperabilità previsti;
- deve supportare l'estrazione di parametri, la trasformazione, l'elaborazione di messaggi XML basata su interfacce visuali, su codice e/o su tecnologia XPath, XQuery, XSLT (extract & transform)
- deve essere integrato in un ambiente di sviluppo object-oriented;
- deve supportare transazioni sincrone ed asincrone;

- deve essere possibile analizzare il traffico che passa attraverso l'ESB per fornire servizi di business intelligence in tempo reale;
- deve potersi integrare con tutte le versioni dei principali RDBMS (Oracle, Microsoft SQL Server, Postgres; MySQL, DB2, etc…);
- deve gestire la profilazione degli utenti per ruoli e attributi (RBAC, ABAC);
- deve supportare obbligatoriamente i seguenti standard specifici di settore: WS Security 1.1, WS Policy, WS Addressing, SAML2, LDAP, X.509, XML Signature, XML, API Rest (con payload JSON, XML) ed il protocollo OAuth 2.0 ed eventuali versioni successive in linea con gli attuali standard tecnologici e di mercato;
- sono inoltre considerati ulteriori standard rilevanti al fine della valutazione: WS Trust, XACML, PKI, WS Reliability, WS ReliableMessaging.

5. REQUISITI NON FUNZIONALI

Nel presente capitolo si descrivono le caratteristiche non funzionali che la soluzione di infrastruttura applicativa dovrà soddisfare.

5.1 Aderenza a standard di riferimento

La soluzione dovrà essere aderente ai principali standard di progettazione delle soluzioni definiti dal Piano Triennale della Pubblica Amministrazione. Inoltre, deve essere aderente agli standard previsti in ambito di Sanità Digitale:Health Level Seven (HL7) Clinical Document Architecture (CDA) Release 2, Portable Document Format (PDF) Livello 3 e livello 1 (PDF/A) per la strutturazione e rappresentazione dei contenuti per i domini delle informazioni, dei dati e dei documenti sanitari, così come definiti dai gruppi di lavoro interministeriali e pubblicati sul sito HL7 e www.fascicolosanitario.gov.it;

- Digital Imaging and Communications in Medicine (DICOM) per la gestione delle immagini medicali e relative informazioni;
- Profili «Integrating the Healthcare Enterprise» (IHE) per lo scambio nazionale e transfrontaliero di domini delle informazioni sanitarie e per l'interoperabilità dei sistemi;

Come requisiti migliorativi della fornitura si richiedere l'aderenza a:

- Modelli informativi basati su risorse come Health Level Seven Fast Healthcare Interoperability Resources (HL7 FHIR ©)
- Nuovi approcci alle specifiche di interoperabilità, quali le pertinenti interfacce API (Application Programming Interfaces).

5.2. Certificazioni e normative di riferimento

Per quanto riguarda le principali normative di riferimento, i sistemi dovranno garantire piena rispondenza a quanto previsto dal D.Lgs. 193/2006 e ss.mm. e ii., alle linee guida emesse dal Garante per la Protezione dei Dati e al nuovo regolamento europeo GDPR.

Inoltre, si prevede che gli anonimi e gli pseudonimi dei pazienti dovranno essere gestiti in base alla norma "Regolamento europeo generale sulla protezione dei dati 2016/679".

5.3. Accessibilità e usabilità

I sistemi devono garantire caratteristiche di accessibilità e usabilità, considerando le diverse tipologie di utenti. Inoltre, devono garantire:

- Modalità di autenticazione e profilazione degli accessi;
- Visualizzazione delle informazioni rilevanti per l'ambito operativo dell'utente e limitazione dei dati modificabili/inseribili in base ai diritti dell'operatore autenticato.
- Configurabilità di allarmi e avvisi da parte dell'operatore per segnalare informazioni importanti, come indicato nei capitoli precedenti.
- Meccanismi di logout automatico nel caso in cui l'operatore non effettui transazioni definite per un determinato periodo di inattività. Questi meccanismi devono essere configurabili per definire il tempo di inattività e le tipologie di transazioni che azzerano il tempo di inattività.
- Interfaccia grafica uomo-macchina basata su HTML5 visualizzabile su tutti i browser delle famiglie Mozilla, Chrome, Safari in lingua italiana, intuitiva, di facile uso e di rapida compilazione, in modo da garantire la sicurezza dei pazienti.
- Interfaccia responsive per un'esperienza efficace ed efficiente dell'utente, per gli applicativi per cui è previsto un front-end per gli utenti (es. CDR).

5.4. Efficienza ed efficacia

La ridondanza dei dati deve essere minimizzata per garantire maggiore correttezza e aggiornamento preciso. Un requisito fondamentale delle soluzioni è la loro modularità, che consente di separare le funzionalità specifiche dei diversi ambiti operativi e configurare i dati da visualizzare in base alle autorizzazioni e alla profilazione degli operatori.
Deve essere evitata la possibilità che gli operatori omettano dati fondamentali o li inseriscano in modo incompleto o sintatticamente scorretto mediante controlli su specifici sui campi, da validare con le Aziende sanitarie.
È essenziale che gli applicativi forniscano reportistica su argomenti quali indicatori chiave di processo, incongruenze nei dati inseriti, statistiche sull'utilizzo dell'applicativo, e così via.
Devono prevedere meccanismi per notificare all'utente l'esistenza di una versione nuova e aggiornata di un'informazione nel caso in cui vengano apportate modifiche all'interno delle soluzioni stesse.

5.5. Disponibilità e affidabilità del sistema

La completa disponibilità dei dati dei sistemi oggetto di fornitura deve essere garantita in qualsiasi momento e luogo, anche in caso di malfunzionamento del sistema, dell'infrastruttura di comunicazione o di

altri sistemi applicativi integrati. Non essendo l'infrastruttura hardware, né quella di rete a carico del Fornitore (rif 6.4 Infrastruttura tecnologica), il proponente dovrà descrivere un'architettura applicativa che, completamente ridondata, consenta, ad esempio, per esigenze di manutenzione ordinaria o straordinaria di escludere componenti/moduli senza creare disservizi all'utenza finale. Il Fornitore è tenuto a presentare una soluzione tecnica atta a garantire la completa disponibilità, come descritto qui sopra, nel rispetto delle indicazioni dell'Agenzia per la Cybersicurezza Nazionale per quanto riguarda la gestione di dati critici.

Essendo i sistemi oggetto dell'appalto fondamentali per rendere interoperabili i processi clinico-assistenziali delle aziende, è di cruciale importanza avere tali servizi sempre disponibili ed attivi, perciò il fornitore dovrà fornire un piano di Business continuity o Disaster recovery ottimale al fine di ripristinare i sistemi nel minor tempo possibile.

Le prestazioni offerte devono rispettare i livelli di servizio previsti in Accordo Quadro, nonché quelli specificati al capitolo 9 del presente documento.

5.6. Tracciabilità ed esibizione

Gli applicativi devono garantire la tracciabilità, tramite log centralizzato, di tutte le operazioni eseguite, come l'accesso, la visualizzazione, l'inserimento, la modifica o l'importazione di dati. Questa tracciabilità deve includere informazioni come la data, l'ora e l'autore dell'operazione, e deve essere registrata attraverso appositi sistemi di log accessibili solo al personale autorizzato.

Deve fornire inoltre degli strumenti atti ad evidenziare situazioni anomale sui singoli sistemi (es. un utente accede ai dati di un paziente troppo frequentemente).

5.7. Licensing

Come stabilito dalla direttiva del 19 Dicembre 2003, ove possibile, le componenti devono basarsi su tecnologie open o, in alternativa, vanno garantite le licenze d'uso proprietarie fornite a tempo illimitato (perpetuo) e con titolarità a favore dell'ente appaltatore. La fornitura deve includere la licenza d'uso dell'intero sistema offerto – compresi eventuali software di terze parti (es. licenze di database, middleware, etc.) – illimitata nel tempo e per un numero illimitato di utenti/sistemi da integrare, consentendo l'utilizzo del software senza limitazioni e senza costi aggiuntivi per tutte le Aziende Sanitarie del Servizio Sanitario Regionale e alla Regione Umbria.

La licenza deve includere tutti gli aggiornamenti (comprese le major release), le correzioni e le nuove funzionalità del software che saranno rilasciate dal Fornitore durante il periodo di validità del contratto. Si **richiede al Fornitore di specificare tipologia di licenza (es. database, prodotto ecc.) e importo per tipologia di licenza**.

5.8. Garanzia

Il Fornitore dovrà fornire a corredo della documentazione tecnica un elenco di tutti i componenti software i quali dovranno avere una garanzia "full-risk" per l'intero periodo di fornitura. Durante tale periodo dovranno essere rispettate le seguenti condizioni:

- manutenzione preventiva;
- tutti gli interventi di manutenzione e/o riparazione dovranno essere effettuati a carico del Fornitore senza alcun onere aggiuntivo.

Il Fornitore garantisce i materiali, i software e le integrazioni fornite da tutti gli inconvenienti non derivanti da forza maggiore, per tutto il periodo di fornitura dalla data del superamento del collaudo, alle condizioni sopra riportate. In tale periodo, salve le maggiori responsabilità sancite dall'art.1669 c.c., il Fornitore è tenuto ad eliminare, a proprie spese, tutti i difetti manifestatisi o guasti nei beni forniti, dipendenti o da vizi di costruzione o sviluppo o configurazione o da altre cause.

5.9. Interoperabilità ed integrazioni

I sistemi oggetto della fornitura dovranno essere integrati in maniera completa. Pertanto, il Fornitore dovrà sviluppare le integrazioni tra gli applicativi oggetto della fornitura, sfruttando il Digital Integration HUB regionale, qualora non avesse già previsto integrazioni dirette tra i singoli applicativi oggetto della fornitura, mediante modalità standard di scambio dati e documenti e in conformità ai profili di integrazione presenti, in ogni caso in coerenza con il framework di comunicazione nazionali ed internazionale IHE, ad esempio HL7 v2.c, HL7 V2+, HL7 v3 ecc.

Il Digital Integration Hub (DIH) ha il compito di esporre i servizi sanitari in maniera uniforme, sicura e controllata. L'accesso ai servizi sanitari regionali verrà mediato dal DIH che si occuperà anche di implementare, se necessario, eventuali logiche di integrazione recuperando i dati dai diversi sistemi regionali. In altre parole, il DIH costituisce la porta di accesso ai sistemi regionali in modo che le integrazioni fra i sistemi esterni alla Regione ed i sistemi regionali siano tracciate, controllate e siano realizzate utilizzando le stesse logiche e livelli di sicurezza.

Il Fornitore dovrà altresì predisporre ed esporre, per ogni sistema oggetto della fornitura, le API REST per:

- l'accesso ai dati gestiti dall'applicativo (dominio applicativo) che consentano di ricercare, inserire, aggiornare, cancellare, modificare e recuperare i dati presenti;
- la gestione dell'applicativo (Management API) tramite le quali effettuare le principali operazioni sul sistema (es. gestione utenti, gestione ruoli, verifica stato sistema "Health check").

Di seguito vengono riportate le integrazioni minime necessarie per gli applicativi oggetto della fornitura:

Master Patient Index (MPI):

- deve integrarsi come slave con l'Anagrafe Regionale Assistiti (ARA), sistema master e gateway, per reperire i dati anagrafici degli assistiti/assistibili gestiti su ARA. Le integrazioni dovranno avvenire utilizzando API REST, API FHIR o messaggi HL7 v.2.5; le modalità di integrazione per i diversi flussi verranno indicate da PuntoZero;
- deve allinearsi con ARA in modalità sincrona;
- deve integrarsi con l'Anagrafica Nazionale Assistiti (ANA) per reperire i dati di assistiti non regionali per mezzo dei servizi esposti da ARA (che sarà utilizzato come gateway) ed implementare i servizi per il recupero e la verifica delle anagrafiche tramite codice fiscale e/o altri dati anagrafici (es. nome, cognome, data di nascita ecc);
- deve essere integrato con il Identity & Privacy Management (IPM);
- deve essere integrato con il DTS
- deve esporre dei web services e canali per l'integrazione con middleware di integrazione e i sistemi di terze parti;
- deve supportare il profilo IHE PDQ, la messaggistica HL7 versione 2.5/2.6 e FHIR;
- deve supportare i seguenti profili IHE: PIX, PIXV3, PIXm, PDQV3, PDQm e XCPD.

Per la USL 1 e per l'AO di Perugia dovranno altresì essere sviluppate:

- le integrazioni che permettano di collegare l'MPI locale esistente con quello regionale oggetto della fornitura per la gestione del periodo transitorio (capitolo 6.3)
- tutte le integrazioni necessarie per poter dismettere l' MPI locale

Anagrafica centralizzata degli Operatori (ACO):

- deve essere integrato con il modulo Identity & Privacy Management (IPM), oggetto della presente fornitura.
- deve essere integrato con il DTS

Identity & Privacy Management (I&PM):

- deve essere integrato con l'MPI
- deve essere integrato con la ACO
- deve essere integrato con il DTS
- deve essere integrato con il CDR

Data Terminology Server (DTS)

Dovrà essere possibile l'integrazione con il DTS nazionale, in fase di realizzazione da parte di AgID/DTD, per la sincronizzazione delle codifiche.

Middleware di integrazione

Sia il middleware oggetto della fornitura, per la USL 2 e l'AO di Terni, che quelli esistenti (e che rimarranno) in uso presso la USL 1 e l'AO di Perugia dovranno essere integrati con il DIH regionale per poter accedere ai servizi esposti dagli applicativi centrali oggetto della fornitura.

La Fornitura deve garantire inoltre, per gli applicativi di seguito riportati, la loro interoperabilità con il FSE 2.0. A tale scopo, le soluzioni devono rispondere ai requisiti dettati dalla normativa di riferimento, tra cui le Linee Guida per l'Attuazione del Fascicolo Sanitario Elettronico (cfr. Fascicolo Sanitario Elettronico 2.0: pubblicate le Linee Guida per l'attuazione | Agenzia per l'Italia digitale (agid.gov.it)). I moduli della fornitura che dovranno garantire il colloquio con FSE 2.0 sono:

- CDR: per l'alimentazione del FSE 2.0
- IPM: per la verifica delle policy di accesso ai dati/documenti presenti in FSE 2.0
- DTS: per la sincronizzazione delle codifiche utilizzate con il DTS nazionale in fase di realizzazione da parte di AgID/DTD

Inoltre, il Fornitore dovrà assicurare la piena interoperabilità degli applicativi oggetto di fornitura con i **sistemi sanitari verticali presenti,** attraverso lo sviluppo di apposite API e fornendo le specifiche di integrazione nei tempi utili di cui si riporta un elenco degli applicativi con maggiore priorità per l'integrazione (anche in riferimento al Modello EMRAM – rif. 5.11):

- CUP
- ADT
- CCE di ricovero e ambulatoriale
- Terapia farmacologica
- Pronto soccorso
- Percorso chirurgico
- RIS/PACS
- LIS
- Sistema trasfusionale (SIT)
- Anatomia patologica
- Radioterapia (per USL 1 e AO Perugia)
- Altri ulteriorii verticali di cartelle/applicativi (es. healthmeeting)

Si configurano come priorità secondaria le integrazioni che i fornitori dei sistemi di terze parti dovranno realizzazione verso l'oggetto di fornitura, a titolo esemplificativo:

- Atl@ante
- COT
- Vaccinazioni
- Infrastruttura regionale di telemedicina (non disponibili ad oggi specifiche tecniche)

5.10. Migrazione dei dati pregressi

Nell'ambito della fornitura si richiede la migrazione dei dati pregressi dai repository aziendali verso il nuovo CDR. Si riserva in fase di analisi di valutare la fattibilità nei tempi di progetto della migrazione dai repository FSE 1.0 verso nuovo il CDR. Saranno comunque da prevedere all'interno della fornitura le integrazioni per garantire l' interoperabilità del nuovo CDR con il FSE 2.0 (cap.5.9).

5.11. La valutazione della maturità digitale delle Aziende con il modello HIMSS EMRAM

Il Ministero della Salute - Unità di missione per l'attuazione degli interventi del PNRR – Ufficio di coordinamento della gestione:

- ha richiamato gli incontri istituzionali tra il Ministero della Salute e i Soggetti Attuatori e ha evidenziato l'importanza del *verification mechanism* del *target* M6C2-8, basato sull'acquisizione del *summary document* di un esperto indipendente;
- al fine di garantire la raccolta del predetto *summary document*, ha dato atto della «*necessità di procedere ad una valutazione del livello di digitalizzazione delle strutture attraverso l'attivazione di idonee procedure/protocolli di verifica validati, nello specifico la Certificazione Electronic Medical Record Adoption Model (EMRAM) – della società Healthcare Information and Management Systems Society (HIMSS);*
- sulla base di quanto sopra, ha avviato una specifica rilevazione del livello di digitalizzazione delle strutture sede di DEA di I e II livello, richiedendo alle Regioni la compilazione di apposito *format*.

In linea con le indicazioni fornite dal Ministero della Salute, la Regione ha individuato il Modello HIMSS EMRAM quale metodo di valutazione del livello di digitalizzazione delle strutture sanitarie operanti a livello regionale.

In questo contesto, la realizzazione di componenti unitarie a livello regionale, oggetto della presente fornitura, rappresenta un elemento strategico e imprescindibile per il raggiungimento degli obiettivi di potenziamento della digitalizzazione posti dal PNRR, per incrementare il patrimonio informativo regionale di ambito sanitario e per implementare i nuovi scenari di integrazione tra i servizi ospedalieri e territoriali, anche in ragione del conseguimento degli obiettivi delineati nel PNRR, in cui il modello EMRAM funge appunto da strumenti di valutazione dell'efficacia globale delle iniziative destinate ai DEA di primo e secondo livello.

Il Modello HIMSS EMRAM è uno strumento riconosciuto e ampiamente diffuso a livello internazionale, unico e indipendente, utilizzato come benchmark per misurare la maturità nell'utilizzo di tecnologie digitali da parte di molteplici strutture ospedaliere.

Data la rilevanza di tale modello nella valutazione della maturità digitale delle Aziende Sanitarie e nella verifica del raggiungimento del target M6C2-8, il Fornitore dovrà garantire che la/e soluzione/i applicativa realizzata nell'ambito della presente procedura, sia coerente con gli standard di qualità e con gli indicatori di digitalizzazione previsti dal modello HIMSS EMRAM per ottenere il finanziamento previsto.

6. ARCHITETTURA DI RIFERIMENTO

6.1 Il Programma Attuativo dell'Ecosistema di servizi di sanità digitale 2023-2026

Il Programma Attuativo dell'Ecosistema di servizi di sanità digitale 2023-2026 (di seguito "Programma"), definito in raccordo con Il "Master-plan della Regione Umbria per la semplificazione e l'agenda digitale 2023-2025" (d'ora in poi Master-plan), definisce **l'architettura di alto livello dell'Ecosistema per i servizi di sanità digitale**, realizzata con l'obiettivo di consolidare gli investimenti sostenuti nel passato, favorendo una logica di evoluzione e upgrade tecnologico, ma anche sfruttare sinergie organizzative e tecniche, nonché economiche, che deriveranno da **un'architettura che centralizza alcuni dei servizi strategici, come appunto la componente di infrastruttura applicativa** e altri applicativi (es. RIS/PACS, VNA, SIT, LIS, Anatomia patologica).

6.2 Modello di Architettura target di alto livello

Viene presentata nel seguito l'architettura target di alto livello, abilitante l'ecosistema dei servizi per la sanità e descritte le componenti strategiche per l'evoluzione dell'ecosistema stesso.

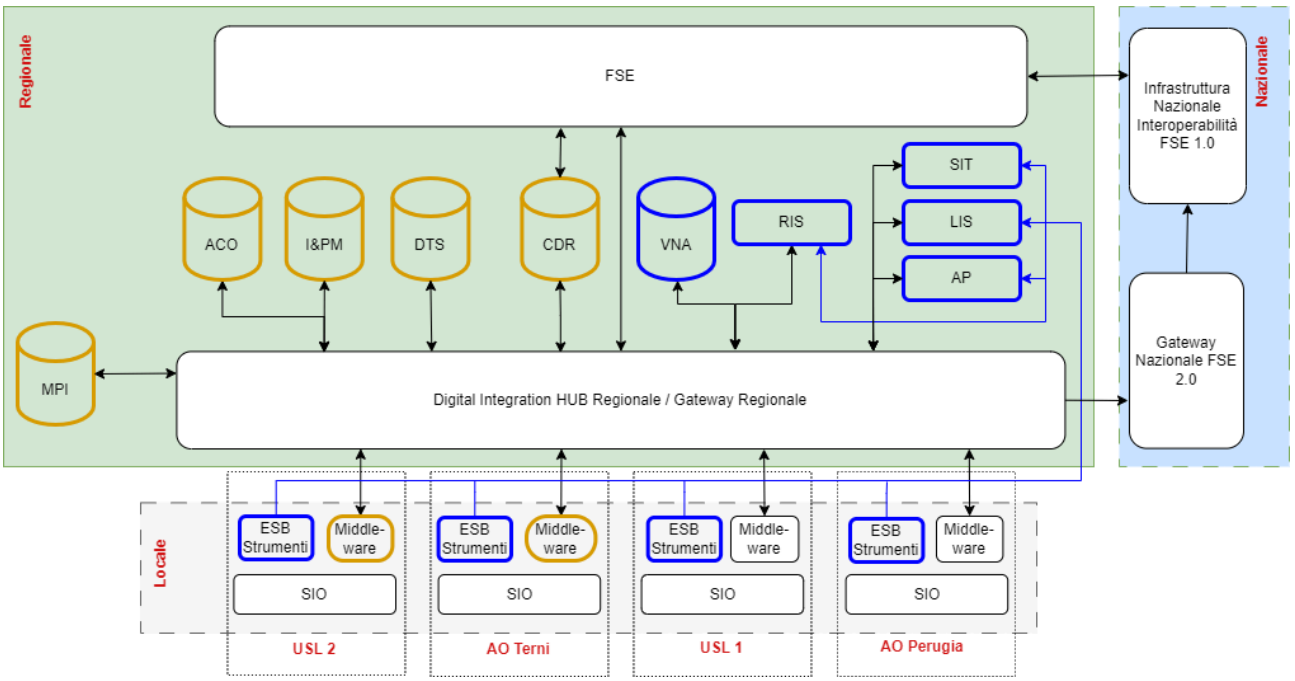

Figura: Architettura di alto livello abilitante l'ecosistema dei servizi per la sanità

Sono rappresentati in giallo nella Figura sopra presentata gli applicativi oggetto della presente fornitura e che vengono descritti nel seguito:

- **Anagrafiche centralizzate - Master Patient Index (MPI)**: la nuova architettura definita prevede un'anagrafica principale dei pazienti (MPI) a livello regionale, gestita in modo centralizzato. Questo comporta la migrazione degli ID pazienti presenti sugli MPI locali, ove presenti, e/o all'interno degli applicativi delle USL/AO verso MPI centralizzato e un progressivo adeguamento in termini di integrazioni di altre componenti applicative (CUP, ADT, CCE, ecc.), per tutte le Aziende. Gli applicativi presenti già a livello centrale (regionale) e i nuovi da realizzare (es. diagnostici) si appoggeranno su MPI Centrale.
- **Anagrafica Centrale Operatori (ACO):** la nuova architettura definita prevede un'anagrafica degli operatori centralizzata a livello regionale, alimentata dalle anagrafiche del personale gestite con il sistema di gestione del personale Sigma, in cui vanno introdotte anche figure non dipendenti (es. praticanti, specializzandi, medici a gettone, etc.).
- **Clinical Data Repository (CDR):** La nuova architettura definita prevede un Clinical Data Repository centralizzato. Il CDR deve favorire la condivisione dei dati tra gli attori (ospedale e territorio), tramite accessi controllati, e permettere di integrare e standardizzare, in modo principalmente strutturato ma anche non strutturato, le informazioni. Il CDR dovrà integrarsi, tramite middleware regionale, con il gateway nazionale per la validazione dei documenti e la successiva pubblicazione su FSE2.0. Il middleware regionale esporrà, per i servizi di validazione e pubblicazione, le stesse API del gateway nazionale.
- **Identity & privacy management (I&PM):** l'Identity Privacy Management è essenziale per garantire un accesso controllato ai dati clinici dei pazienti nel CDR, in base alle scelte di privacy e consensi rilasciati dagli stessi. In prospettiva, permettere l'accesso controllato, basandosi sui ruoli e i permessi degli utenti, ai dati clinici dei pazienti da parte di qualsiasi applicativo del SIO.
- **Data Terminology Server (DTS):** la nuova architettura prevede di dotarsi di un DTS per centralizzare la gestione applicativa delle codifiche, garantendo l'interoperabilità semantica, che permette di definire standard di codifica e terminologia comuni che possono essere utilizzati da diversi applicativi o sistemi all'interno di un'organizzazione sanitaria, anche quando usati riferimenti terminologici diversi all'interno degli applicativi.
- **Middleware di integrazione:** la nuova architettura definita prevede un digital integration hub (DIH) a livello regionale per gestire le integrazioni verso le componenti centralizzate e layer locali (delle Aziende) di integrazione, in modo da consentire l'interscambio da e verso le applicazioni non centralizzate di ASL e AO, per cui è prevista la progressiva migrazione verso Cloud della PA Idoneo o PSN per i servizi critici, in coerenza con le indicazioni di ACN. **E' oggetto della presente fornitura solo il middleware locale per la USL 2 e Azienda Ospedaliera di Terni**. Il middleware locale dovrà garantire la continuità operativa e interfacciarsi con il DIH. Nello schema sono inoltre rappresentati gli ESB (ESB strumenti) per le integrazioni degli strumenti di laboratorio e diagnostica, *non oggetto della presente fornitura.*

Sono rappresentati in blu nella Figura sopra rappresentata gli applicativi a carattere regionale per cui è previsto un upgrade tecnologico o nuova realizzazione sempre nell'ambito dell'investimento M6C2 I.1.1.1 Ammodernamento del parco tecnologico e digitale ospedaliero – Digitalizzazione DEA di I e II livello (rif. 2.3 Iniziative correlate) e che vengono descritti nel seguito:

- **Radiology Information System – Picture Archiving and Communication System (RIS-PACS) e VNA**: la nuova architettura mira ad unificare e potenziare i sistemi di gestione delle immagini diagnostiche, noti come RIS e PACS, per creare una struttura regionale centralizzata. L'obiettivo principale è ottimizzare il flusso di lavoro nel processo diagnostico ospedaliero e migliorare l'integrazione tra strutture sanitarie, seguendo una visione strategica regionale.

  Per quanto riguarda il RIS, il piano prevede un aggiornamento avanzato attraverso la piattaforma Elefante.net, che permetterà alle Aziende Sanitarie di pianificare e razionalizzare le attività diagnostiche lungo tutto il percorso del paziente. Per quanto riguarda il PACS, si prevede un avanzamento attraverso la piattaforma Enterprise Imaging for Radiology. Un altro obiettivo è l'unificazione dei database dei sistemi RIS nelle quattro Aziende coinvolte, per creare un sistema RIS regionale con anagrafica unificata. Questo favorirebbe l'attivazione di servizi di teleconsulto, ridurrebbe gli esami ripetitivi, ottimizzerebbe le risorse e diminuirebbe i tempi di attesa. Infine, è prevista l'ottimizzazione del sistema di gestione delle dosi di radiazioni e il monitoraggio dei materiali radioattivi presso le strutture sanitarie, al fine di garantire la sicurezza dei pazienti e del personale medico nell'uso delle tecnologie diagnostiche e terapeutiche.

  La nuova architettura prevede l'introduzione di un repository clinico centralizzato (vendor Neutral archive-VNA) per l'archiviazione di contenuti multimediali, e quindi il consolidamento di tutto il patrimonio iconografico aziendale in un archivio, in modo che ogni reparto/struttura abbia la possibilità di visualizzare le informazioni generate in altre strutture, nel rispetto dei ruoli e permessi degli utenti.

- **Sistema Trasfusionale territoriale (SIT):** la nuova architettura prevede la creazione di un sistema informatico centralizzato, in logica cloud, per la gestione dei Servizi di Immunoematologia e Trasfusionale (SIT). Lo sviluppo e centralizzazione degli attuali applicativi avverrà tramite l'evoluzione della soluzione Emodata di Tesi, attualmente implementata nell'Azienda Ospedaliera di Perugia, Azienda Ospedaliera di Terni e USL Umbria 1. La medesima soluzione applicativa sarà diffusa anche presso l'Azienda USL Umbria 2 che attualmente dispone di un software per la gestione del trasfusionale dell'azienda Mesis.

  Il nuovo sistema informativo regionale dei servizi trasfusionali si pone l'obiettivo di facilitare e coordinare la gestione di tutti i processi svolti all'interno di una rete trasfusionale, come l'organizzazione della raccolta di sangue, la gestione dei donatori, le fasi di prelievo, conservazione, lavorazione e validazione del sangue, la distribuzione di sangue intero, emocomponenti ed emoderivati. Il sistema consentirà inoltre di raccogliere in modo efficiente i dati relativi a ciascun processo, ai fini di effettuare elaborazioni statistiche ed agevolare la condivisione di informazioni epidemiologiche e di attività. La soluzione sarà composta da diversi moduli funzionali. In particolare, sarà previsto un modulo per la gestione dei donatori, un modulo per la gestione delle trasfusioni, un modulo per la gestione delle cellule staminali ed un modulo per la gestione del sistema qualità, rischio clinico e per la gestione della documentazione.

- **Laboratory Information System (LIS):** la nuova architettura mira ad unificare i sistemi di gestione dei servizi di laboratorio analisi delle diverse aziende per realizzare una singola piattaforma cloud che permetta il raggiungimento dei seguenti obiettivi:

· Facile interscambio di campioni tra punti prelievo e laboratori, gestendo tutta la tracciabilità del campione nelle fasi di pre-analitica, analitica e analisi con visione e tracciamento dell'avvenuta lettura da parte del medico richiedente;

· Condivisione delle best practice a livello regionale, tra cui ad esempio la condivisione tra le diverse aziende delle regole di sistema di regole esperto per regolare l'appropriatezza prescrittiva delle richieste d'esame pervenute dai sistemi richiedenti;

· Funzionalità di telelaboratorio e teleconsulto, permettendo quindi, nel rispetto delle policy di sicurezza aziendali e del GDPR, il lavoro a distanza e la collaborazione tra i laboratoristi delle diverse aziende;

· Monitoraggio delle prestazioni di efficacia ed efficienza dei diversi laboratori;

· Gestione dei consensi e delle richieste di oscuramento ed anonimizzazione;

· Elevata disponibilità della soluzione con ridondanza applicativa sul cloud;

· Maggiore resilienza dei servizi di laboratorio analisi regionali nel momento in cui, per cause di forza maggiore, venisse a mancare l'operatività di uno o più laboratori. Sarà possibile attivare con procedure standardizzate il reindirizzamento e trasporto delle richieste di analisi verso laboratori limitrofi.

Tale attività di implementazione della nuova soluzione applicativa di carattere regionale si colloca anche nel progetto di riorganizzazione e razionalizzazione della rete dei laboratori analisi promossa dalla Regione Umbria, come decretato dalla DGR 617/2023 "Approvazione del modello organizzativo della Rete dei Laboratori Analisi della Regione Umbria". Il nuovo modello organizzativo dei laboratori viene descritto nell'Allegato 1 della DGR 510/2022 e prevederà 2 centri HUB, 5 centri spoke e 7 centri P.O.C.T.

- **Anatomia patologica (AP):** la nuova architettura prevede di unificare l'applicativo di Anatomia Patologica (AP) e promuovere l'avvio del progetto di Digital Pathology (DP), al fine di creare una piattaforma regionale integrata unica, accessibile agli anatomopatologi dell'Umbria ed esterni. Il progetto mira al raggiungimento dei seguenti obiettivi:

· Gestione dell'anagrafica degli utenti, accesso e gestione dei 'casi' per professionisti esterni con possibile anonimizzazione. Saranno previste funzionalità di 'superuser' per l'assegnazione dei 'casi', garantendo un accesso sicuro in conformità con il GDPR;

· Integrabilità con altri sistemi ospedalieri tramite standard HL7 per la gestione dei 'casi', archiviazione e gestione dell'URL delle immagini acquisite. La soluzione di DP sarà accessibile

tramite chiamata di contesto dal gestionale di AP, integrandosi con lo stesso per l'acquisizione dell'assegnazione dei casi;

· Acquisizione di immagini per vetrini storici con associazione manuale al paziente. Sarà possibile associare più immagini a un 'caso', aggiungere nuove immagini con assegnazione automatica dei casi, e visualizzare e validare le immagini. Saranno inclusi l'utilizzo di algoritmi di intelligenza artificiale, il download delle immagini e la gestione dello storage delle immagini;

· Disponibilità di un visualizzatore per l'analisi e la refertazione dell'immagine relativa a un vetrino. Sarà implementato un sistema di visualizzazione a bassa e alta risoluzione per le immagini, con funzionalità di confronto e analisi comparativa;

· Generazione di report completi con tutte le informazioni inserite a sistema per il caso in esame. Saranno disponibili reportistica e/o dashboard per il monitoraggio delle attività;

· Disponibilità di un help desk online per il supporto all'utente, con classificazione delle immagini attraverso metadati e tag per ricerche personalizzate.

Inoltre, nello schema sono evidenziati l'FSE (Fascicolo Sanitario 2.0) ed il Digital Integration HUB regionale:

- **FSE 2.0:** è costituito dal registry, con gestione dell'Affinity Domain Italia, e dallo strato di integrazione con L'Infrastruttura Nazionale di Interoperabilità (National Gateway dell'FSE 1.0) per il colloquio con le altre regioni. FSE 2.0 di Regione Umbria, oltre ai nuovi servizi necessari per FSE 2.0, garantisce il funzionamento in interoperabilità interregionale (da e verso le altre regioni) di tutti i servizi previsti da FSE 1.0:

  - Ricerca documenti e recupero riferimenti documento
  - Recupero documento
  - Comunicazione metadati
  - Trasferimento dei metadati
  - Gestione informative e modulistica di acquisizione consenso
  - Gestione consenso

  FSE verrà progressivamente adeguato dalle specifiche previste per FSE 1.0 a quelle per FSE 2.0; l'adeguamento prevede i seguenti passaggi:

  - realizzazione delle nuove API conformi alle specifiche del gateway per FSE 2.0
  - realizzazione ulteriori API per i servizi di ricerca e recupero documenti
  - adeguamento dei sistemi alimentanti con produzione dei documenti in formato PDF firmato PAdES con allegato il CDA2 in modalità ATTACHMENT
  - adeguamento dei sistemi alimentanti per l'integrazione mediante le nuove API FSE 2.0

- Integrazioni dei sistemi alimentanti non ancora integrati con FSE 1.0 (vaccinazioni, produttori referti di specialistica ambulatoriale, ecc.).

- **Digital Integration HUB:** Il layer di integrazione è basato su una logica a microservizi. In particolare, il componente di integrazione espone un set di API analoghe a quelle del gateway nazionale attraverso le quali i sistemi produttori potranno inviare dati e documenti (formato CDA2) al CDR. Le stesse API verranno esposte al CDR per il colloquio con il gateway nazionale.

L'architettura target sopra descritta dovrà essere realizzata attraverso interventi che tengano in considerazione un periodo transitorio (par. 6.3) che vedrà un'evoluzione del contesto applicativo ad oggi presente.

6.3 Gestione della fase transitoria verso l'architettura target

La **realizzazione dell'infrastruttura applicativa** presentata all'interno dell'architettura di alto livello (rif. 6.2), oggetto della presente fornitura, dovrà **tenere in considerazione per la sua realizzazione, l'evoluzione del contesto applicativo** che porterà alcuni interventi su soluzioni locali per le Aziende Sanitarie, congiuntamente alla messa a disposizione di servizi comuni/applicativi di carattere regionale.

Per dare maggiore evidenza all'Aggiudicatario del **contesto della fase transitoria**, viene rappresentata nel seguito la **situazione attuale (as-is) dell'infrastruttura applicativa**, e dei sistemi che saranno oggetto di sostituzione/upgrade tecnologico, e i **relativi interventi del transitorio** che includono appunto la realizzazione della presente fornitura e delle iniziative a carattere regionale (RIS/PACS e VNA, LIS, SIT e AP), per abilitare il Modello di architettura a tendere (6.2).

SITUAZIONE AS-IS

La situazione per i diversi applicativi oggetto della fornitura è la seguente:

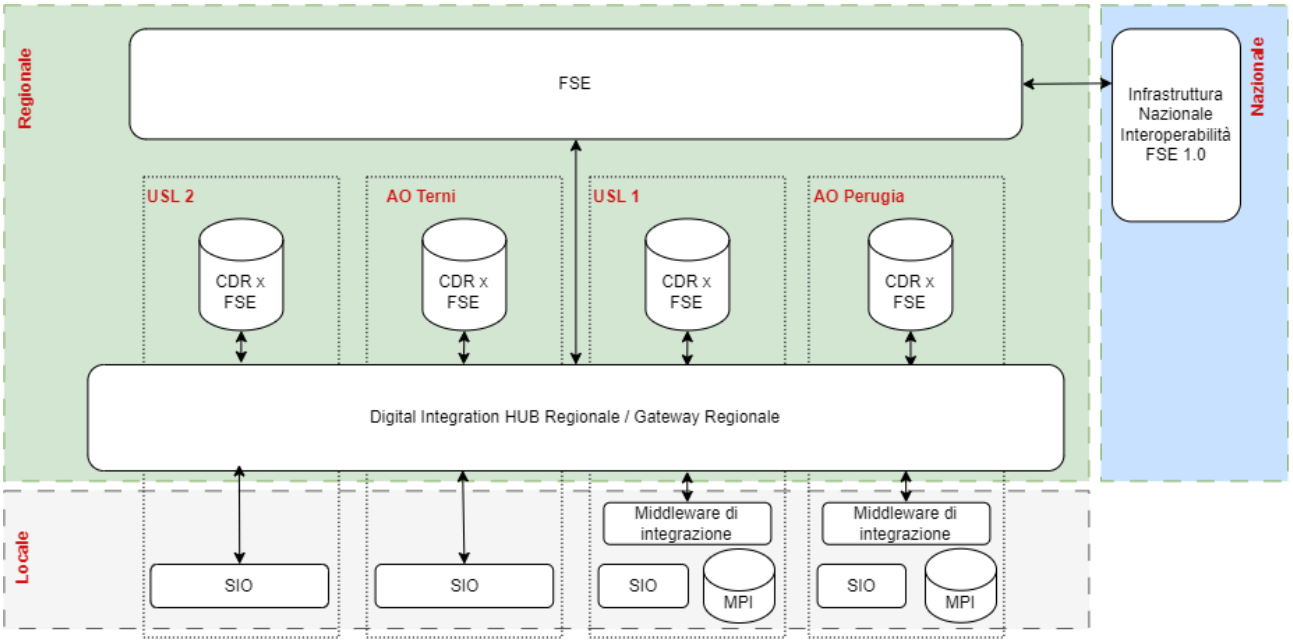

Figura: Architettura logica AS-IS

a) Anagrafiche centralizzate - Master Patient Index (MPI)

Attualmente, all'interno di Regione Umbria, non esiste un sistema di Master Patient Index (MPI) centralizzato a livello regionale. Sono presenti due diverse anagrafiche: l'Anagrafe Sanitaria Regionale basata su MDBWEB di Engineering e un'anagrafe derivata utilizzata dalla piattaforma SAR per la diffusione delle informazioni ai Medici di Medicina Generale (MMG) e ai Pediatri di Libera Scelta (PLS).

Nel contesto specifico delle strutture sanitarie dell'Umbria, l'USL Umbria 1 e l'Azienda Ospedaliera (AO) di Perugia hanno sviluppato il proprio MPI locale. Tuttavia, vi sono alcuni punti di attenzione per l'integrazione di questi sistemi con altre applicazioni. Ad esempio:

- USL Umbria 1: Soltanto alcuni applicativi sono integrati con l' MPI locale come ad esempio Galileo (Cartella Clinica Elettronica), FirstAid (Pronto Soccorso), Ormaweb (Percorso Chirurgico), RIS/PACS e servizi di telemedicina/gruppi multidisciplinari tramite Healthmeeting. L' MPI è anche integrato con anagrafica SOGEI per cercare e certificare tramite il codice fiscale, le anagrafiche di pazienti non regionali. Il sistema ADT (GPI Lisa) non è tra gli applicativi connessi con MPI ed utilizza una sua anagrafica che viene aggiornata dall' anagrafe sanitaria regionale (MDBWEB) tramite un job automatico giornaliero.

- Azienda Ospedaliera di Perugia: ha integrato numerosi applicativi del mondo Dedalus, inclusi CCE Galileo, FirstAid, Ormaweb e servizi di telemedicina tramite C4C Picasso mentre non sono stati integrati i sistemi RIS/PACS, il laboratorio di analisi e il sistema di ADT (GPI).
- L'USL 2 e l'Azienda Ospedaliera di Terni non dispongono di un sistema MPI.

b) Anagrafica Centrale Operatori (ACO)

Regione Umbria non dispone di una anagrafe unica degli operatori sanitari di riferimento. Sino ad oggi le necessità di informazioni relative agli operatori sanitari delle strutture pubbliche sono state soddisfatte attingendo agli applicativi di gestione del personale delle Aziende, sia del personale dipendente che convenzionato. Gli applicativi che necessitano di tali informazioni sono dotati in genere di una anagrafe locale che consente di soddisfare le esigenze specifiche. Esiste, in fase di dispiegamento, un sistema di gestione del personale Sigma, in cui vanno introdotte anche figure non dipendenti come ad es. praticanti, specializzandi, medici a gettone, etc.

c) Identity and Privacy Management (IPM)

Non è presente un IPM centralizzato.

d) Clinical Data Repository (CDR)

Il CDR è implementato attualmente utilizzando una piattaforma suddivisa in 5 istanze separate, una per i Profili Sanitari Sintetici prodotti da MMG/PLS, ed una associata ad ogni specifica Azienda Ospedaliera (AO) o Unità Sanitaria Locale (USL) nella regione. Il CDR così implementato alimenta il FSE 1.0 (in corso di evoluzione verso FSE 2.0), il flusso per la consegna dei referti ai MMG/PLS e supporta il flusso per l'archiviazione sostitutiva dei documenti che è stato realizzato ma non attivato in ambiente di produzione. Il CDR supporta l'alimentazione tramite messaggi HL7 v.2.5 (MDM-T02, MDM-T10 e MDM-T11) e tramite messaggi IHE XDS.b (ITI-41 per la pubblicazione ed ITI-42 per l'indicizzazione). L'interrogazione del CDR avviene mediante standard IHE XDS.b (ITI-18 per la ricerca dei documenti e ITI-43 per il recupero dei documenti).

e) Data Terminology Server (DTS)

Non è presente un DTS centralizzato che consenta di centralizzare la gestione delle codifiche, garantendo l'interoperabilità semantica.

f) Middleware di integrazione locale

L'attuale situazione del Middleware di integrazione locale è caratterizzata da una varietà di soluzioni utilizzate a livello delle diverse strutture e a livello regionale:

- USL Umbria 1 e AO di Perugia utilizzano un middleware. Questa soluzione funge da intermediario tra diverse applicazioni e sistemi, facilitando lo scambio di dati e l'integrazione tra di essi.
- USL Umbria 2 e AO Terni non hanno un middleware locale che gestisce l'interoperabilità dei sistemi.

La situazione per i diversi applicativi a carattere regionale è la seguente:

RIS/PACS: attualmente, il sistema RIS utilizza Elefante.Net (versione 2.79) presso vari Enti Sanitari. L'Azienda Ospedaliera di Perugia ha installato Elefante.Net nel 2019, mentre l'USL Umbria 1 nel 2021. Inoltre, l'Azienda Ospedaliera di Terni e l'USL Umbria 2 utilizzano applicativi diversi per la gestione radiologica.

Per quanto riguarda il PACS, gli attuali sistemi PACS variano tra le diverse Aziende Sanitarie:

- L'Azienda Ospedaliera di Perugia utilizza il sistema Impax (versione 6.6) con visualizzatore Xero.

- L'Azienda Ospedaliera di Terni utilizza Impax (versione 6.6).

- L'USL Umbria 1 utilizza Impax (versione 6.5 e 6.6) e Enterprise Imaging (versione 8.2) per alcuni presidi.

- L'USL Umbria 2 utilizza Impax e Sectra per la gestione dello screening mammografico.

Non è presente un VNA.

SIT : Il Sistema trasfusionale attualmente in uso presenta funzionalità limitate ed aggiornamenti obsoleti, ad oggi presenta soluzioni applicative eterogenee sul territorio Umbro con omogeneità applicativa per quanto riguarda la USL Umbria 1, e le due Aziende Ospedaliere presenti sul territorio.

LIS: Il sistema LIS attualmente in uso presso le aziende Umbre è un sistema on premise presso i data center locali delle aziende, nonostante la soluzione applicativa sia omogenea sul territorio, che presenta criticità da un punto di vista di sicurezza e di performance.

AP: Attualmente, solo l'Azienda Ospedaliera di Perugia è dotata di dispositivi per la digitalizzazione dei vetrini (es. scanner e monitor) e presenta un'esperienza di Digital Pathology.

INTERVENTI DEL TRANSITORIO

Il primo intervento di infrastruttura applicativa deve consentire di portare le quattro aziende ad un livello comune per quanto riguarda l'interoperabilità a livello locale, prevedendo l'installazione e configurazione del middleware di integrazione locale per la USL Umbria 2 e l'AO di Terni.

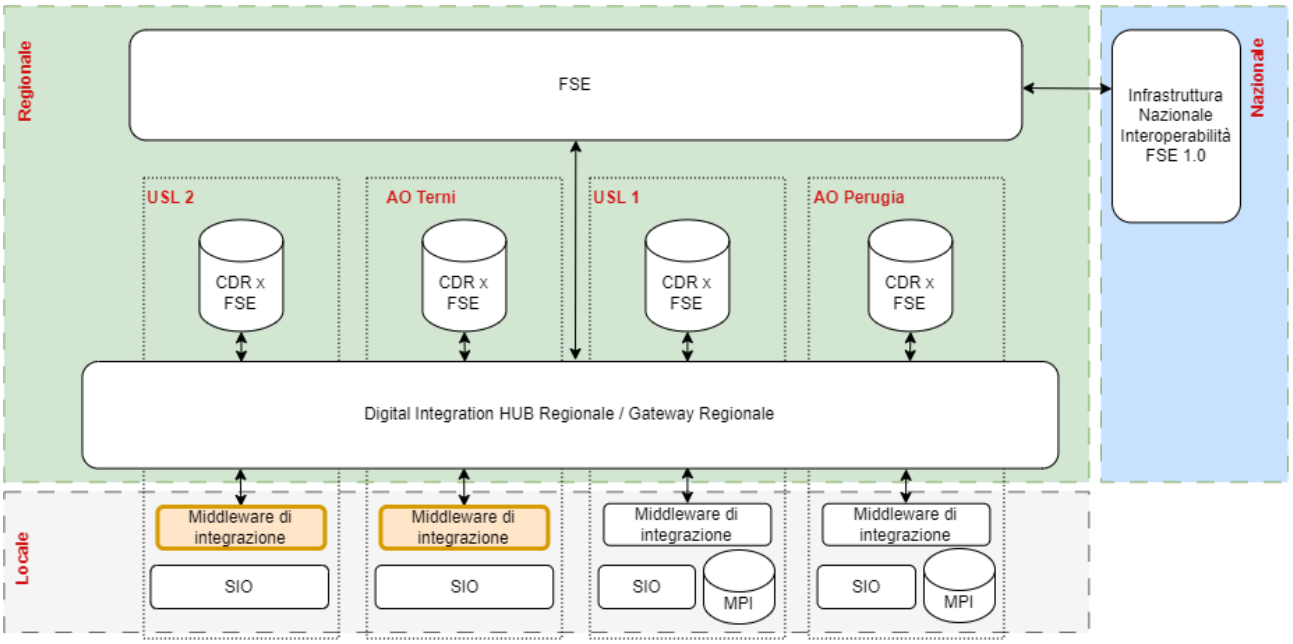

Figura: Transitorio con Inserimento Middleware locale USL Umbria 2 e AO Terni

Gli interventi successivi/paralleli alla realizzazione del middleware di integrazione locale riguardano le altre componenti in perimetro della presente fornitura: MPI, ACO, I&PM, DTS e CDR a livello regionale (*Figura: Architettura transitoria verso i nuovi moduli centralizzati*), comprensivo delle installazioni, configurazioni e integrazioni necessarie.

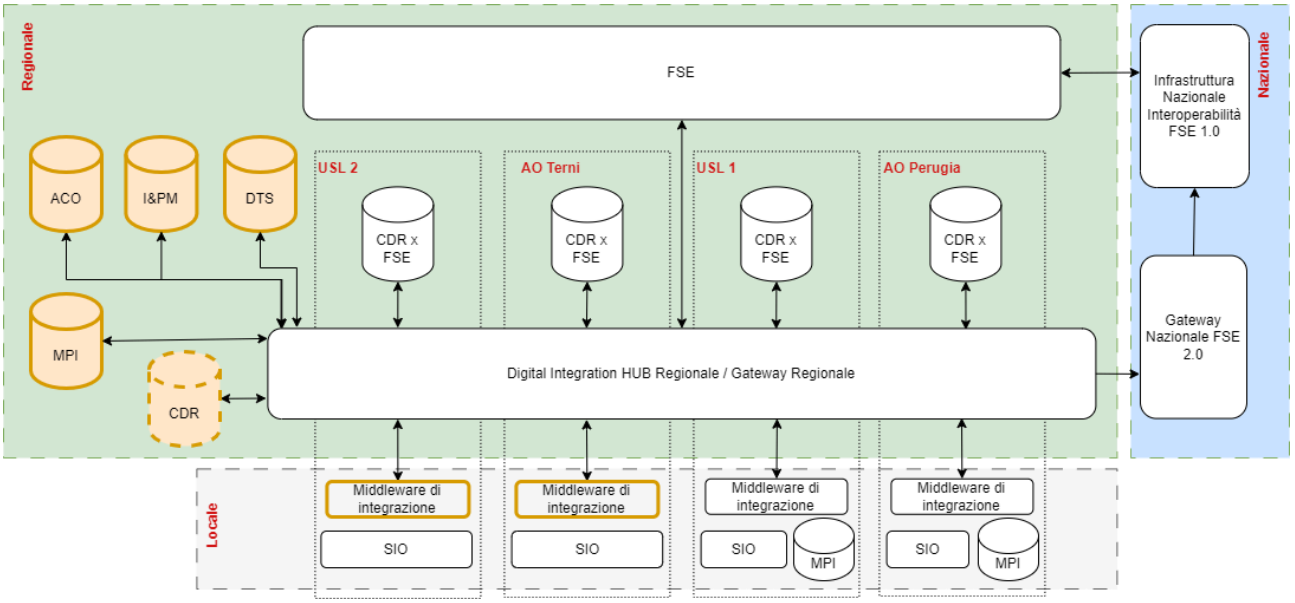

Figura: Architettura transitoria verso i nuovi moduli centralizzati

E' mandatorio per il Fornitore progettare e avviare la realizzazione delle suddette componenti secondo **un piano coerente con il contesto applicativo e che tenga in considerazione la propedeuticità anche con le nuove componenti centralizzate** da realizzare o per cui è previsto un upgrade tecnologico (es. LIS, RIS/PACS e VNA ecc).

a) Master Patient Index (MPI)

Propedeutico all'installazione del MPI ed all'integrazione dello stesso all'interno dell'architettura regionale è l'analisi ed attuazione di un piano di popolamento del sistema che preveda l'inserimento delle anagrafiche dei due MPI presenti, in USL Umbria 1 ed AO di Perugia, e di tutte le anagrafiche locali dei moduli presenti nei sistemi informativi dei quattro enti (USL e AO) che non risultano integrate con gli attuali MPI locali in uso sul MPI regionale. Prima di procedere al popolamento del MPI regionale con le suddette anagrafiche, dovrà inoltre essere attuata una normalizzazione dei dati anagrafici estratti dai diversi sistemi eliminando le anagrafiche duplicate e/o errate. È fondamentale che il fornitore verifichi che tutte le chiavi prelevate dai vari applicativi corrispondano univocamente ad un'unica posizione segnalando tempestivamente qualsiasi anomalia al fine di poter bonificare le posizioni errate. A titolo di esempio vengono presentati due workflow applicabili durante la fase transitoria.

Il primo è il workflow, che sarà in uso presso gli enti che attualmente non hanno la disponibilità di un MPI locale, descrive ad alto livello i passaggi necessari per il reperimento di un ID anagrafico da parte di un applicativo locale (nell'esempio in Figura si fa riferimento al Pronto Soccorso).

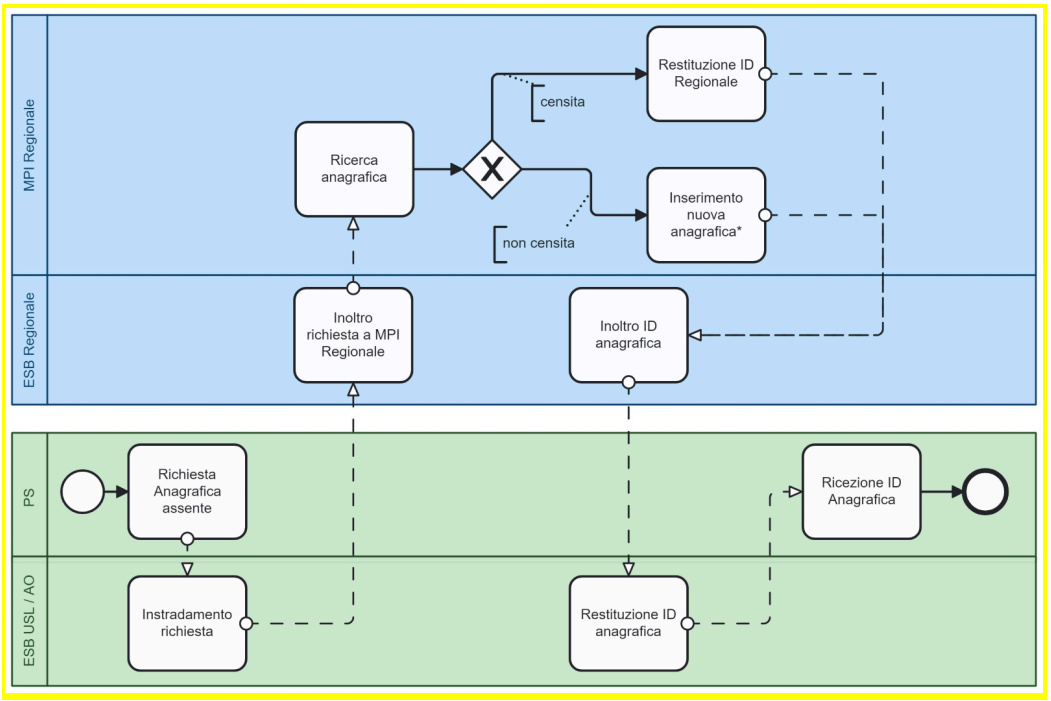

Figura : Applicativo locale richiede ID anagrafica

Il secondo esempio (Figura sottostante) descrive ad alto livello lo stesso flusso per gli enti che hanno la disponibilità di un MPI locale.

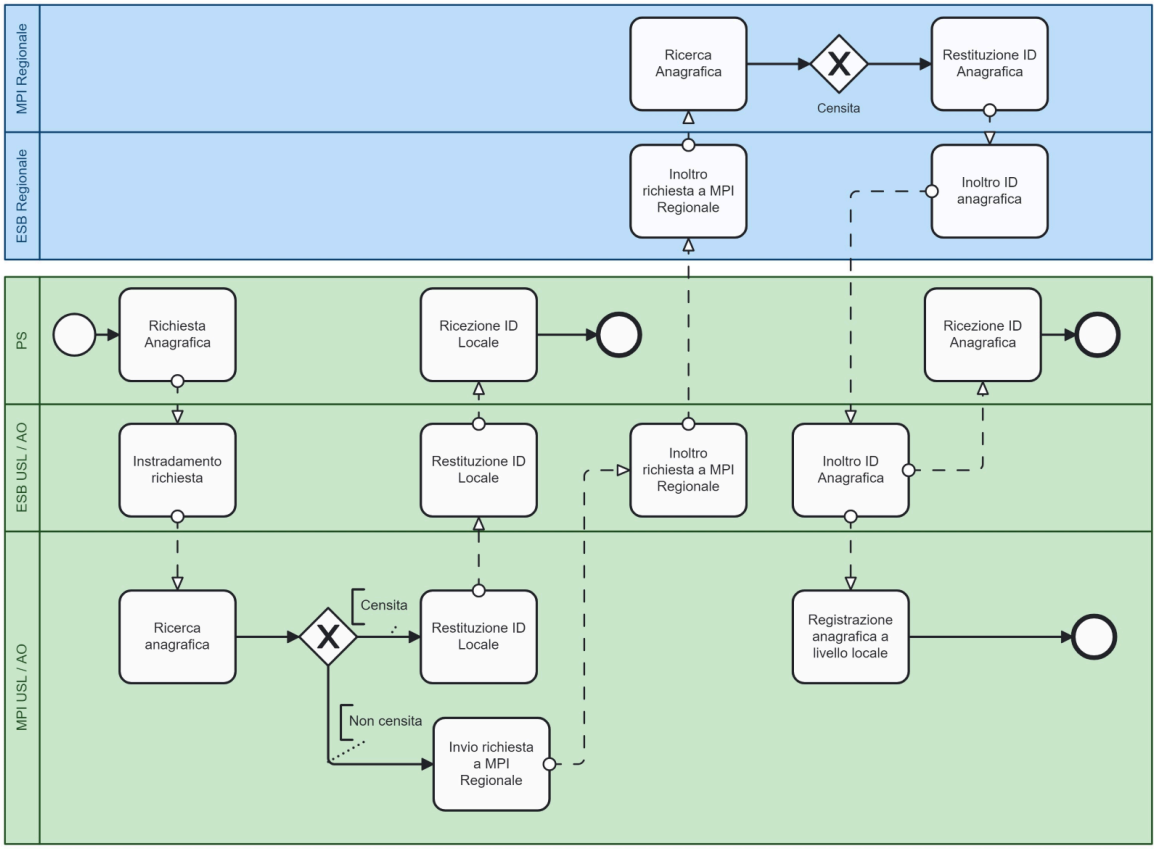

Figura: Applicativo locale richiede ID anagrafico tramite MPI locale

Anche per i due enti che hanno al momento un MPI locale dovrà essere applicato il nuovo workflow previsto per le due aziende che non hanno attualmente un MPI locale. **Si ribadisce che all' interno del periodo transitorio dovranno essere dismessi gli attuali MPI locali in uso presso Usl Umbria 1 ed AO Perugia, migrando i verticali a loro collegati, verso l' MPI regionale**. Parallelamente all' installazione del middleware locale in USL Umbria 2 ed AO Terni, il fornitore dovrà prevedere quindi un piano di azione coerente con le tempistiche del transitorio e secondo le indicazioni delle aziende appaltanti, per migrare tutti i verticali collegati agli MPI locali delle Aziende USL Umbria 1 ed AO Perugia al nuovo MPI regionale.

b) Anagrafica Centrale Operatori (ACO)

In questa fase si dovrà provvedere al popolamento del database della ACO prelevando le informazioni dal sistema del personale SIGMA, che è in fase di dispiegamento, e procedere con le attività di installazione, configurazione e sviluppo.

c) Identity & Privacy Management (I&PM)

Per la configurazione dell'I&PM è necessaria la preventiva disponibilità dell'ACO. È necessario, inoltre, che vengano analizzate le regole di accesso ai dati in uso sugli attuali sistemi e si effettui una riorganizzazione e normalizzazione delle stesse per la parametrizzazione a livello regionale dell'accesso ai dati dei pazienti.

d) Data Terminology Server (DTS)

Dovranno essere caricate le principali codifiche nazionali ed internazionali; dopo l'analisi delle codifiche utilizzate dai diversi enti si dovrà procedere al loro caricamento sul DTS e alla relativa mappatura rispetto alle codifiche nazionali ed internazionali disponibili come, ad esempio: SNOMED, LOINC, ICD-9-CM, ICD-10-CM ecc., nel rispetto dei requisiti funzionali indicati al presente capitolato. Per maggiori dettagli si faccia riferimento al capitolo dei Requisiti funzionali.

e) Clinical Data Repository (CDR)

Nella fase transitoria dovrà essere configurato il nuovo CDR con partizioni logiche per ciascuna azienda/ente ma resteranno comunque attivi gli attuali CDR. Il nuovo CDR dovrà implementare le modalità di alimentazione tramite messaggi HL7 v2.5, transazioni IHE ITI-41, API FSE 2.0 e garantire il collegamento con FSE per l'indicizzazione dei documenti. Le integrazioni esistenti degli applicativi verticali dovranno essere progressivamente migrate dagli attuali CDR al nuovo CDR.

In parallelo agli interventi sopra indicati, viene condotto l'adeguamento tecnologico vero FSE2.0, *che non è oggetto della presente fornitura*, che per l'anno 2024 prevede l'integrazione del FSE di Regione Umbria con il Gateway Nazionale e l'adeguamento alle Linee Guida FSE 2.0 per gli applicativi che producono le seguenti tipologie di documenti:

- Referti di Laboratorio
- Referti di Radiologia
- Lettere di Dimissione Ospedaliera
- Verbali di pronto Soccorso
- Referti di Anatomia Patologia
- Referti di Specialistica Ambulatoriale
- Profili Sanitari Sintetici

In particolare, gli applicativi indicati dovranno:

- Produrre i documenti in formato PDF con allegato il CDA2 in modalità attachment

- Firmare i documenti con firma di tipo PAdES
- Accreditarsi con il DTD per garantire la conformità dei documenti prodotti alle linee guida FSE 2.0
-

Al termine del periodo transitorio descritto ad alto livello in questo capitolo, l'architettura dei sistemi dovrà essere come rappresentata nel Modello di Architettura di alto livello (rif. 6.2).

Si richiede al Fornitore di presentare **un piano degli interventi per la realizzazione dei sistemi oggetto della presente fornitura per abilitare l'architettura target, in coerenza con le progettualità correlate a carattere regionale**; resta inteso, tuttavia, che il Fornitore stesso deve provare, con qualsiasi mezzo appropriato nell'offerta tecnica, che quanto proposto ottempera in maniera equivalente e/o superiore ai requisiti/obiettivi definiti nel presente capitolato tecnico.

Il Fornitore dell'infrastruttura applicativa dovrà interfacciarsi e coordinarsi, anche direttamente, con i Fornitori aggiudicatari delle procedure di approvvigionamento dei sistemi centralizzati per garantire la gestione della fase transitoria senza generare impatto sugli utenti finali, limitando al minimo i disservizi, nonché con gli attuali fornitori degli applicativi che dovranno interfacciarsi con i servizi di infrastruttura applicativa.

6.4 Infrastruttura tecnologica

La soluzione dovrà presentare un'architettura web-based.

Lo *standard* architetturale di riferimento dovrà essere quello di Applicativo *Multi-tenant* che in sintesi prevederà:

- **Architettura *Multi-Tenant*** e segregazione degli ambienti e governo degli accessi a garanzia delle "titolarità" dei dati.
- ***Cloud Native*:**
  - La soluzione dovrà essere *Cloud Native*, ossia sviluppata e progettata per poter operare su infrastruttura cloud.
- ***Linee Guida AgID*:**
  - La soluzione proposta (sia strutturale sia concettuale) deve essere modellata tenendo conto del principio di *Privacy by design*, ovvero quell'approccio ingegneristico che si concentra sull'intero processo di tutela della *privacy* e che segue i sette principi su cui si basa:
    - Proattivo non reattivo, preventivo non correttivo;
    - *Privacy* come impostazione predefinita;

- *Privacy* incorporata nella progettazione;
- Piena funzionalità - somma positiva, non somma zero;
- Sicurezza *end-to-end* - Tutela dell'intero ciclo di vita;
- Visibilità e trasparenza;
- Rispetto per la *privacy* degli utenti.

Inoltre, nello sviluppo del software, devono essere tenute in considerazione le “linee guida per lo sviluppo del software sicuro” pubblicate da Agid.

La soluzione proposta, in tutte le sue componenti, dovrà essere installabile sia "on-premise" nei data center regionali basati sulla suite di virtualizzazione VMWare vCloud Foundation 8, che in cloud su CSP (Cloud Service Provider) qualificati da ACN per la gestione di dati e servizi di livello critico.

L'installazione della soluzione on-premise o su CSP qualificato sarà valutata sulla base dell'architettura proposta e la disponibilità delle componenti infrastrutturali necessarie all'implementazione.

6.5 Requisiti e vincoli

Il sistema di infrastruttura applicativa oggetto di fornitura dovrà soddisfare i seguenti requisiti:

- mantenere le applicazioni allineate alle nuove versioni dei prodotti/framework utilizzati, ovvero l’applicazione non dovrà utilizzare versioni di prodotti prossimi a “end-of-life” e/o “end-of-support”;
- gestire adeguatamente la tracciatura degli eventi (log audit);
- gli aggiornamenti o eventuali release del sistema devono essere effettuati senza provocare interruzioni del servizio;
- garantire elevate performance anche in presenza di elevati carichi di lavoro;
- garanzia di Elevata disponibilità del Servizio, anche a fronte di failure di singole componenti.

In riferimento all’architettura sopra riportata, per quanto possibile, occorre rimanere il più aderenti possibile al modello proposto da HL7 per quanto riguarda l’infrastruttura FHIR, in particolare devono essere sfruttate le RESTFul API senza operare cambi di paradigma implementativo

La verifica della compatibilità della soluzione per il rilascio verrà effettuata in sede di valutazione del Documento Progettuale di Dettaglio (DPD). I sistemi dovranno essere sviluppati nel rispetto delle linee guida, strumenti e metodologie definite dall’Open Web Application Security Project (OWASP).

Il **Fornitore è tenuto a descrivere nell’offerta tecnica la specifica tecnica delle risorse di calcolo necessarie all’implementazione e corretta gestione del sistema**. Al fine di poter garantire la corretta efficienza nell’utilizzo delle risorse di calcolo messe a disposizione da PuntoZero s.c.a.r.l, in fase di erogazione del servizio si terrà conto dell’opportuno dimensionamento delle risorse richieste dal Fornitore tramite gli

appositi LdS definiti nel capitolo 9.5. Durante il periodo di fornitura, il dimensionamento proposto dal Fornitore verrà analizzato a cadenza trimestrale tramite i report che dovranno essere realizzati dal Fornitore e sottoposti ad approvazione da parte di PuntoZero s.c.a.r.l.. 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 a PuntoZero s.c.a.r.**l.**

BUSINESS CONTINUITY E DISASTER RECOVERY

La completa disponibilità dei dati dei sistemi oggetto di fornitura deve essere garantita in qualsiasi momento e luogo, anche in caso di malfunzionamento del sistema, dell'infrastruttura di comunicazione o di altri sistemi applicativi integrati. Il Fornitore dovrà descrivere un'architettura applicativa che, completamente ridondata e resiliente al di là della componente infrastrutturale, consenta, ad esempio, per esigenze di manutenzione ordinaria o straordinaria di escludere componenti/moduli senza creare disservizi all'utenza finale. Il Fornitore è tenuto a presentare una soluzione tecnica atta a garantire la completa disponibilità, come descritto qui sopra, nel rispetto delle indicazioni dell'Agenzia per la Cybersicurezza Nazionale per quanto riguarda la gestione di dati critici.

Essendo i sistemi oggetto dell'appalto fondamentali per rendere interoperabili i processi clinico-assistenziali delle aziende, è di cruciale importanza avere tali servizi sempre disponibili ed attivi, perciò il fornitore dovrà fornire un piano di Business continuity o di Disaster recovery ottimale, al fine di avere sia i sistemi sempre attivi, che di ripristinare i sistemi nel minor tempo possibile.

Inoltre, devono essere adottati meccanismi che consentano di assegnare manualmente degli identificatori provvisori nei casi in cui i sistemi di contesto non siano reperibili (es. Pronto Soccorso per inserimento anagrafiche in emergenza), con possibilità di reintegro delle informazioni, tramite opportune integrazioni, afferenti alle richieste d'esame una volta ripristinati tali sistemi.
Le prestazioni offerte devono rispettare i livelli di servizio previsti in Accordo Quadro, nonché quelli specificati al capitolo 9 del presente documento.

BUSINESS CONTINUITY

La completa disponibilità dei dati delle singole soluzioni oggetto della fornitura deve essere garantita in qualsiasi momento e luogo, anche in caso di malfunzionamento del sistema, dell'infrastruttura di comunicazione o di altri sistemi applicativi integrati dell'Azienda Sanitaria. Il fornitore dovrà garantire, per quanto di sua competenza, la business continuity (BC) del servizio - ai sensi dell'art. 50-bis del Codice dell'Amministrazione Digitale, intesa come piano d'insieme delle procedure e soluzioni tecnico-organizzative, accorgimenti e delle misure di reazione e risposta a eventi imprevisti che possono compromettere, anche parzialmente, all'interno o all'esterno dell'organizzazione, il normale funzionamento dei servizi ICT utilizzati per lo svolgimento delle funzioni istituzionali. Il Piano di Emergenza e di Continuità Operativa deve essere presentato in sede di proposta. Inoltre, i sistemi devono adattarsi e seguire le

procedure di emergenza e continuità operativa dell'Azienda Sanitaria e in accordo con il Cloud service provider.

DISASTER RECOVERY

Il Fornitore deve:

- assicurare il servizio di copia e allineamento dei dati dei sistemi primari con i dati contenuti nei sistemi secondari;
- garantire la manutenzione della soluzione di BC/DR e delle componenti software che compongono la cosiddetta configurazione di emergenza, assicurando i servizi per la riattivazione e il ripristino dei sistemi primari/di produzione a seguito di una condizione di emergenza;
- garantire i seguenti tempi massimi di ripristino del sistema: RTO = 30 min e RPO = 30 min, essendo gli applicativi oggetto della fornitura strategici ai fini dell' interoperabilità tra i vari sistemi informativi sanitari;
- porre in essere ogni attività di sua competenza per i test periodici previsti per la verifica della corretta funzionalità delle soluzioni adottate per garantire la soluzione di Disaster Recovery, evitando di compromettere i dati di produzione durante le simulazioni e predisponendo copie dei dati a uso esclusivo della simulazione stessa da cancellare al termine delle prove. L'effettuazione del test deve essere concordata con le relative Strutture Sanitarie e Cloud service provider. Nel caso in cui il test non dovesse dare esito positivo, l'Aggiudicatario si impegna a ripetere il test in accordo, si impegna altresì a risolvere le criticità evidenziate, per quanto di sua competenza, restando a suo carico ogni onere derivante dalle predette attività comprese le responsabilità da ciò derivanti.

I livelli di servizio sono indicati nel presente capitolato (cap. 9).

7 SERVIZI PROFESSIONALI

L'iniziativa dovrà essere accompagnata da una gamma di servizi professionali di natura tecnica e gestionale atti a supportare la transizione al nuovo servizio, nonché orientati alla efficace operatività della soluzione stessa.

7.1 Servizi applicativi

***Project management* dell'iniziativa**: rientrano in queste attività il coordinamento gestionale e amministrativo dell'iniziativa complessiva ed il supporto agli enti nella gestione dei singoli cantieri di lavoro per tutta la durata dell'iniziativa.

Analisi, Progettazione, installazione, configurazione, sviluppo e collaudo delle soluzioni oggetto di fornitura: rientrano in queste attività l'analisi, progettazione, installazione, configurazione, sviluppo ed integrazioni, collaudo sul contesto umbro dei servizi e soluzioni applicative facenti parte della fornitura in oggetto. Queste attività riguarderanno il periodo dall'inizio della Fornitura al termine del transitorio di attivazione del nuovo sistema. In particolare, tali attività riguarderanno:

- La definizione delle specifiche funzionali e di interfaccia;
- La definizione delle specifiche di interfaccia verso i sistemi informativi esterni;
- La definizione delle specifiche tecniche del software;
- La realizzazione del software;
- I test e collaudi delle componenti software.

Servizi di integrazione tra gli applicativi oggetto della fornitura, nonchè sviluppo di web services da esporre per consentire l'integrazione verso gli oggetti della fornitura degli applicativi del Sistema Informativo delle Aziende. All'interno del perimetro della Fornitura sono comprese le attività specialistiche lato Fornitore volte all'integrazione della soluzione.

Dispiegamento e supporto alla messa in esercizio e altri Servizi Gestionali Connessi al governo delle installazioni: rientrano in queste attività tutti quei servizi di supporto alla fase di messa in esercizio della soluzione, della formazione e diffusione dei sistemi, del supporto operativo alla attivazione del sistema e del governo complessivo del sistema, tra cui il supporto alla gestione della Domanda, alla pianificazione delle implementazioni e delle evoluzioni, alla diffusione della soluzione, ai servizi per la gestione del cambiamento e la formazione e supporto tecnico-specialistico alle Aziende. Particolare attenzione dovrà essere riservata a supportare le singole Aziende nella fase di transizione al nuovo sistema e rispetto alle iniziative correlate (rif. 6.3). In particolare, si richiede al Fornitore di:

- Individuare, in base alle esigenze degli utenti, le migliori soluzioni alle problematiche emerse;
- Definire le check-list di verifica per le funzionalità rilasciate;
- Definire con le Aziende i piani dettagliati degli interventi, in coerenza con gli altri interventi di digitalizzazione dei DEA (iniziative correlate) previsti con la descrizione delle attività unitamente alla durata e alle date previste di fine lavoro.
- Fornire il supporto alle validazioni;
- Organizzare e svolgere il **servizio di formazione** per tutti gli utenti degli applicativi oggetto di fornitura e per i servizi ICT;
- Organizzare e svolgere il servizio di **supporto operativo all'avvio** per il tempo necessario;

Manutenzione, Assistenza e Supporto conduzione applicativa: rientrano in queste attività i servizi di manutenzione (correttiva ed adeguativa) del software in esercizio e l'assistenza a tutti gli utenti della soluzione in oggetto, a partire dal completamento della prima attivazione della Fornitura alle Aziende fino al termine del contratto. Si ritengono inclusi in questa classe di servizi, il servizio di gestione applicativi e basi dati che comprende l'insieme di attività, risorse e strumenti di supporto per la gestione delle applicazioni, delle loro relative basi dati e data services e l'assistenza (help desk di I e II livello). Inoltre, sono inclusi gli aggiornamenti tecnologici (comprese le major release) del sistema fornito rilasciati nel corso della durata della Fornitura. Tenendo conto della criticità dei servizi oggetto di fornitura, il fornitore dovrà essere in grado di garantire una elevata capacità di intervento e fornire prestazioni documentabili.

Supporto infrastrutturale: rientrano in queste attività i servizi infrastrutturali finalizzati alla presa in carico e messa in esercizio delle infrastrutture HW nonché l'attività di Help Desk di 2 livello finalizzata alla risoluzione delle problematiche legate all'utilizzo delle infrastrutture in conduzione.

Gestione operativa delle installazioni, Tuning, Monitoraggio della soluzione: rientrano in queste attività tutti i servizi di manutenzione, assistenza ed esercizio della soluzione sia nella sua versione originaria sia con le eventuali personalizzazioni, aggiornamenti e implementazioni introdotti nel tempo a partire dal completamento della prima attivazione della Fornitura agli ES fino al termine del contratto.

Pianificazione e realizzazione delle evoluzioni dei servizi: rientrano in queste attività tutti i servizi di vera e propria evoluzione della soluzione complessiva e dei servizi correlati, intesi come sviluppo di nuovi sistemi e/o funzionalità specifiche (ad es. sviluppo di software ad hoc), che potranno essere richieste dagli enti.

Exit Strategy: alla scadenza del contratto il Fornitore dovrà garantire l'assistenza necessaria a trasferire la gestione dei servizi oggetto di fornitura alle Aziende o ad una terza parte da esse individuata.

7.2 Servizi applicativi a richiesta

Rientrano in questi servizi:

-**Servizio di manutenzione evolutiva** che comprende gli interventi di evoluzione delle funzionalità e delle componenti dell'architettura applicativa e gli interventi atti ad introdurre nel sistema corrente nuove funzionalità, volte a migliorare il livello di interoperabilità sanitaria. Per l'erogazione di tale servizio vengono stimate per la USL 2 circa 100 giornate (GG/team ottimale) lungo tutta la durata del contratto.

-**Supporto specialistico** per esempio per gestire le attività di integrazioni che gli applicativi delle aziende dovranno effettuare verso oggetti infrastruttura applicativa . Il servizio comprende attività di supporto con la finalità di assicurare risposte specialistiche per indirizzare le scelte tecnologiche e opportunità di ottimizzazione dell'infrastruttura. Sono attività 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 (Sviluppo Software Ex-novo, Evoluzione Applicazioni Esistenti, Adeguamento, Configurazione e Personalizzazione) ma anche ai servizi di Gestione e Migrazione.

I servizi sopra descritti potranno essere realizzati su richiesta dell'ente Regionale e degli ES, che si riserva la facoltà di richiederne l'effettiva attivazione solo dopo aver valutato la risposta tecnica/economica del Fornitore. Il Fornitore sarà infatti tenuto a rispondere alla richiesta di intervento proponendo un progetto di lavoro e la stima dell'impegno necessario, che saranno oggetto di validazione da parte dell'ente Regionale.

7.3 Profili professionali

I profili professionali, per l'erogazione dei servizi riportati nel presente Capitolo, saranno oggetto di valutazione da parte delle Aziende, il quale potrà valutare il curriculum della risorsa e potrà effettuare un

colloquio per valutarne l'aderenza delle competenze con quanto richiesto nel presente Capitolato Tecnico e con le finalità dell'attività da svolgere.

I curricula vitae dei profili professionali da impiegare nei vari servizi dovranno essere resi disponibili alle Aziende, rispettando lo schema di CV Europeo. In ogni caso, dovranno essere particolarmente dettagliate le competenze/conoscenze/esperienze tecniche al fine di verificare la corrispondenza con i requisiti minimi, e gli eventuali requisiti migliorativi offerti.

Resta salva la facoltà delle Aziende di richiedere sostituzione, dandone adeguata motivazione, di una risorsa in qualsiasi momento, in questo caso il Fornitore dovrà garantire il subentro di una nuova risorsa secondo i Livelli di servizio definiti.

Per usufruire di tali servizi le Aziende potranno scegliere di disporre delle seguenti profili professionali:

- Project Manager;
- ICT Business Analyst;
- Healthcare Solution Specialist;
- Healthcare Data Scientist;
- Cloud Application Architect;
- Cloud Application Specialist;
- Cloud Security Specialist;
- Devops Expert;
- Enterprise Architect;
- System Integration & Testing Specialist;
- Developer (Cloud / Front-End / Mobile);
- Database Specialist & Administrator;
- Systems & Network Administrator;
- User Experience Designer;
- Digital Media Specialist – Mobile;
- Digital Media Specialist – Publishing;
- Service Desk Agent.

Le risorse richieste potranno svolgere le proprie attività presso la sede dell'ES o in modalità remota sulla base delle esigenze esposte dal richiedente. La giornata lavorativa della risorsa dovrà essere intesa come una giornata di 8 ore consecutive (fatta salva la pausa pranzo) dalle 8:00 alle 18:00, dal lunedì al venerdì.

Relativamente alle caratteristiche richieste per tipologia di profilo si prega di far riferimento a quelle esplicitate all' Appendice 1A ("Profili Professionali") Al Capitolato Tecnico Speciale dell'Accordo Quadro CONSIP "Servizi Applicativi in ambito "SANITÀ DIGITALE - Sistemi Informativi sanitari e servizi al cittadino" Per Le Pubbliche Amministrazioni del SSN".

8 REALIZZAZIONE, DIFFUSIONE, GESTIONE, ASSISTENZA E MANUTENZIONE

8.1 Generalità

Il fornitore dovrà organizzare le proprie attività nel rispetto dei vincoli temporali e secondo le modalità di azione descritte a livello generale.

Le suddette attività includono:

- Il monitoraggio puntuale e completamento del programma definito in questa sezione, entro i tempi previsti, incluse le attività di coordinamento delle diverse aree coinvolte;
- Il coordinamento con altri progetti in corso presso gli Enti Sanitari coinvolti e la Regione Umbria al fine di evitare conflitti e gestire le interrelazioni reciproche;
- Elaborazione della struttura organizzativa, delle responsabilità e dei gruppi di lavoro del progetto, favorendo la cooperazione tra il personale degli Enti Sanitari e quello del Fornitore;
- La definizione degli standard e delle procedure comuni per la Forniture con l'obiettivo di assicurare un coordinamento efficace e chiaro, nonché di organizzare sistemi di comunicazione e trasmissione delle informazioni efficienti tra le diverse parti coinvolte nell'iniziativa;
- L'elaborazione di piani operativi, di contingenza e di continuità operativa chiari e dettagliati;
- La gestione adeguata del periodo di transizione, anche in ragione di quanto descritto al capitolo 7, al fine di assicurare la continuità nei processi principali di cura del paziente.

Successivamente all'assegnazione della fornitura, il Fornitore è tenuto a collaborare con gli Enti Sanitari e la Regione Umbria per concordare, formalizzare e condividere documenti di sintesi che definiscano ruoli, responsabilità, funzioni e modalità di comunicazione e interazione tra le parti coinvolte, nel rispetto di quanto definito nel presente Capitolato Tecnico.

Inoltre, per rendere efficienti le attività di gestione e di condivisione delle informazioni il Fornitore deve predisporre un repository documentale dedicato e strumenti per la gestione in formato elettronico della documentazione, del relativo cronoprogramma (generale ed esecutivo di dettaglio) e di ogni documento tecnico di comune interesse (Project Management Information System – PMIS).

8.2 Fasi progettuali e relative tempistiche

La presente sezione contiene le informazioni connesse all'introduzione della nuova infrastruttura applicativa (servizi comuni) per il sistema informativo sanitario della Regione, definendo le principali attività che dovranno essere svolte presso ogni ES, le tempistiche massime e i vincoli a cui il Fornitore dovrà attenersi. **Si sottolinea che le attività di introduzione della nuova soluzione/i dovranno essere svolte garantendo il minor disservizio possibile per operatori e pazienti**. Di seguito sono descritte le attività che il Fornitore sarà tenuto a svolgere per ogni ES in cui inserirà la nuova soluzione oggetto della fornitura:

Di seguito sono riportate le attività che il Fornitore dovrà svolgere per ciascuna Azienda:

- **Elaborazione di un Piano Esecutivo di Progetto** che comprenda l'assessment, la progettazione del sistema e la preparazione dell'avvio.
- **Formalizzazione di un Piano Operativo di Progetto** che riguardi lo sviluppo della singola soluzione e la sua diffusione presso ogni Azienda.
- **Implementazione, test e collaudo** delle soluzioni.
- **Completamento della diffusione** della soluzione, avvio e formazione degli utilizzatori.
- **Gestione a regime** della soluzione.

Durante le attività previste nelle diverse fasi sarà fondamentale il continuo confronto con i referenti dell'ES e della Regione, al fine di mantenere costantemente allineati gli obiettivi dell'intervento con le esigenze raccolte.

Le tempistiche dettagliate per ciascuna attività, a partire dalla data di avvio di progetto che sarà definita dagli enti a seguito della firma del contratto esecutivo, saranno concordate nel documento contrattuale, considerando attentamente le esigenze e le peculiarità di ogni Azienda. In particolare, la tabella seguente riassume le tempistiche previste per le attività:

Tempistiche previsto dall'avvio	Relativa fase progettuale
Entro il 3° mese dalla stipula del contratto	Assessment e preparazione dell'avvio ivi inclusa la formalizzazione di un Piano Esecutivo di Progetto
Entro il 6° mese dalla stipula del contratto	Avvio installazione, configurazione e sviluppo della soluzione e formalizzazione di un Piano Operativo di progetto
Entro il 12°- 15° mese dalla stipula del contratto e, in ogni caso, entro e non oltre la milestone stabilita dal PNRR (giugno 2025)	Realizzazione e collaudo per la messa in esercizio delle soluzioni sulle quattro Aziende Sanitarie coinvolte come da specifiche del presente capitolato tecnico
Fino al termine della fornitura	Gestione a regime delle soluzioni

Il momento di avvio del progetto sarà definito dalle Aziende a seguito della firma del contratto esecutivo.

8.2.1 Assessment e definizione del piano esecutivo di implementazione per l'ES

Nella fase iniziale il Fornitore effettuerà un assessment iniziale dei sistemi informativi attualmente implementati nelle Aziende Sanitarie coinvolte. Questa attività si pone l'obiettivo di comprendere lo stato attuale del patrimonio informativo delle Aziende coinvolte, con un particolare focus sulle modalità di accesso normate dagli scenari applicativi e le integrazioni interne necessarie per mettere in comunicazione le applicazioni oggetto di fornitura, nonché sviluppare i servizi per le integrazioni lato applicativi terzi che compongono il Sistema Informativo dell'ES.

A valle di questa attività, il fornitore è tenuto a produrre due documenti:

- Un **documento di assessment** che includa necessariamente una mappatura di tutti i processi che interessano l'introduzione della nuova soluzione di infrastruttura applicativa, con il coinvolgimento di tutti gli stakeholder, ed una mappatura delle integrazioni presenti tra le applicazioni del Sistema Informativo.
- Il **Piano Esecutivo**, che includa tempi e modi di azione su ciascuna Azienda Sanitaria. Tale documento deve includere, in particolare, il piano delle attività, e relative modalità, previste per l'introduzione della soluzione nel suo complesso, con relative tempistiche necessarie, ed il piano di rollback che includa le specifiche azioni da eseguire in presenza di gravi anomalie, al fine di riportare l'intero Sistema Informativo a una condizione di piena funzionalità.

Entrambi i documenti precedentemente citati dovranno essere condivisi con le Aziende Sanitarie che, in seguito alle verifiche effettuate sulla coerenza dei documenti, potrà accettare la documentazione o richiedere modifiche o integrazioni.

Se le Aziende Sanitarie accettano la documentazione, il Fornitore può avviare le attività operative correlate alla realizzazione progettuale. In caso di richieste di modifiche, le Aziende possono richiedere una revisione dei documenti, formalizzando gli Elementi che non sono coerenti con quanto previsto contrattualmente o rispetto alle modifiche/integrazioni richieste. Si precisa che resta salvo il termine previsto dal Capitolato Tecnico per il completamento della fase, il non rispetto del quale comporta l'applicazione delle relative penali.

Le attività di analisi sopra descritte afferiscono al servizio previsto dall'Accordo Quadro Servizio di *"Sviluppo di Applicazioni Software Ex-novo- Green Field (GF)"*.

8.2.2 Formalizzazione di un Piano Operativo di progetto, installazione, configurazione e sviluppo delle soluzioni

Questa fase prevede le attività di progettazione, previa analisi di cui al 8.2.1., installazione, configurazione, e sviluppo delle soluzioni, incluse le integrazioni necessarie, come esplicitate nel presente documento, e quanto previsto nel Piano Esecutivo precedentemente definito e secondo il Piano Operativo accordato con gli ES/Aziende.

Le attività di questa fase sono da intendersi come comprensive della realizzazione delle integrazioni tra gli applicativi oggetto della fornitura e della realizzazione dei servizi da esporre verso gli applicativi del Sistema

Informativo dell'ES che dovranno integrarsi con le componenti di infrastruttura applicativa, necessarie al corretto funzionamento della soluzione stessa.

Le attività sopra descritte, per tutte le soluzioni oggetto della presente fornitura, afferiscono al servizio previsto dall'Accordo Quadro Servizio di *"Sviluppo di Applicazioni Software Ex-novo- Green Field (GF)"*. Il servizio dovrà essere attivato necessariamente ad inizio contratto e concludersi entro e non oltre la milestone PNRR di Giugno 2025. Si richiede di fornire in sede di offerta tecnica, l'indicazione delle GG/uomo necessarie alla realizzazione dei singoli applicativi oggetto di fornitura, come riportato per il servizio previsto dall'Accordo Quadro Servizio di:

- *"Sviluppo di Applicazioni Software Ex-novo- Green Field - MPI"*
- *"Sviluppo di Applicazioni Software Ex-novo- Green Field - ACO"*
- *"Sviluppo di Applicazioni Software Ex-novo- Green Field - I&PM"*
- *"Sviluppo di Applicazioni Software Ex-novo- Green Field - DTS"*
- *"Sviluppo di Applicazioni Software Ex-novo- Green Field - CDR"*
- *"Sviluppo di Applicazioni Software Ex-novo- Green Field - Middleware"*

Le attività di analisi, configurazione e personalizzazione sul digital integration hub (DIH) - middleware regionale - afferiscono al servizio previsto dall'Accordo Quadro Servizio di *"Configurazione e personalizzazione di Soluzioni di terze parti/open source/riuso"*. Il servizio dovrà essere attivato necessariamente ad inizio contratto e concludersi entro e non oltre la milestone PNRR di Giugno 2025.

8.2.3 Test e collaudo delle soluzioni

La fase di test e collaudo comprende tutte le attività di verifica funzionale e tecnica delle soluzioni per singola Azienda Sanitaria. Il Fornitore dovrà eseguire diverse tipologie di test, che dovranno riguardare tutte le funzionalità della nuova soluzione nel suo complesso.

Prima di iniziare il collaudo, il Fornitore è tenuto a produrre un **Piano di Collaudo** con modalità e tempistiche per ogni applicativo oggetto di fornitura, per ogni tipologia di test, i casi d'uso coperti dal test e le funzionalità impattate.

La tabella sottostante indica i test previsti ed i relativi deliverable che il Fornitore dovrà produrre a seguito delle attività per ogni singolo applicativo oggetto di fornitura e per l'infrastruttura applicativa nel suo complesso.

Tipo di test	Deliverable
Funzionali	Verbale di esecuzione dei test funzionali con il relativo esito

Prestazionali	Verbale di esecuzione dei test prestazionali riportante i servizi e le funzionalità e i tempi di risposta registrati
Processuali	Verbale di esecuzione dei test processuali riportante i processi ed i percorsi organizzativi dell'Azienda
Di sicurezza	Verbale di esecuzione dei test di sicurezza
Di integrazione	Verbale di esecuzione dei test di integrazione
Test di non regressione	Verbale di esecuzione dei test di non regressione
Test del modello fisico della base dati	Verbale di esecuzione dei test del modello fisico della base di dati

In seguito alle verifiche eseguite sul Piano di Collaudo elaborato, l'Azienda Sanitaria potrà

- Accettare il Piano;
- Richiedere delle modifiche/integrazioni.

Nel primo caso il Fornitore potrà avviare le attività operative previste. Nel secondo caso, il Fornitore sarà tenuto a recepire le indicazioni ricevute dall'Azienda ed a presentare nuovamente il Piano entro e non oltre 5 giorni lavorativi. L'Azienda Sanitaria (ES) avrà la facoltà di richiedere una revisione dell'output presentato dal Fornitore, formalizzando eventuali incongruenze con i termini contrattuali o con le modifiche/integrazioni richieste. Si precisa che resta salvo il temine previsto dal Capitolato Tecnico per il completamento della fase, il non rispetto del quale comporta l'applicazione delle relative penali.

Il processo di collaudo sarà condotto con la partecipazione dei referenti operativi sia dell'Azienda Sanitaria che del Fornitore. Tutti i verbali derivanti dalle varie sessioni di test dovranno essere consegnati all'Azienda Sanitaria. In caso di esito negativo in alcuni test, si richiederà la loro ripetizione fino al pieno successo di tutte le prove stabilite. L'avvio dell'operatività regolare della Fornitura presso ciascuna Azienda Sanitaria sarà subordinato al superamento del collaudo e alla verifica dell'adempimento agli obblighi amministrativi ed organizzativi.

Il risultato del collaudo sarà formalizzato attraverso un verbale che riporterà le prove superate e eventuali fallimenti riscontrati, firmato dai referenti operativi coinvolti. A seguito del collaudo saranno attivate le attività per la messa in esercizio delle soluzioni.

Inoltre, l'esito positivo del collaudo nel suo complesso definirà conseguentemente anche i tempi nei quali la soluzione sarà ritenuta sotto garanzia, ovvero nei 12 mesi (come anche citato nel Capitolato Generale

dell'Accordo Quadro CONSIP "Servizi Applicativi in ambito "SANITA' DIGITALE – Sistemi Informativi Sanitari e servizi al cittadino" Per Le Pubbliche Amministrazioni del SSN") successivi al collaudo stesso.

I collaudi delle soluzioni potranno essere organizzati seguendo le logiche ipotizzate nel GANTT allegato "AS_Infrastruttura applicativa_Ipotesi macro gantt", per il quale il fornitore potrà presentare una proposta migliorativa in sede di offerta tecnica.

Le attività sopra descritte, per tutte le soluzioni oggetto della presente fornitura, afferiscono al servizio previsto dall'Accordo Quadro Servizio di "Sviluppo di Applicazioni Software Ex-novo- Green Field (GF)". Il servizio dovrà essere attivato necessariamente ad inizio contratto e concludersi entro e non oltre la milestone PNRR di Giugno 2025.

8.2.4 Formazione e attività di assistenza specialistica

Dopo il collaudo dei sistemi sistema, il Fornitore dovrà avviare iniziative formative e di assistenza specialistica al fine di supportare l'avvio del sistema. Le figure professionali coinvolte nelle attività di formazione dovranno possedere requisiti tecnici adeguati, nonché una specializzazione nell'utilizzo e nella configurazione dei sistemi applicativi forniti e della sua parametrizzazione. Il fornitore dovrà garantire supporto completo all' avvio del sistema, così da assicurare tempestività per la risoluzione di eventuali problemi tecnici. Su richiesta delle quattro Aziende Sanitarie, il supporto potrà essere richiesto anche on-site. Le attività formative saranno concordate con gli Enti Sanitari e pianificate anticipatamente. In particolare, è richiesta la redazione di un Piano di Formazione dettagliato che comprenderà una descrizione delle attività formative programmate, il calendario delle stesse, focalizzandosi sul personale di nuova assunzione e sulla presentazione delle funzionalità applicative. L'offerta formativa erogata sarà personalizzata in base alla tipologia di personale coinvolto. In particolare, la formazione specifica per i servizi ICT e i sistemisti sarà atta alla diffusione di competenze specifiche ed un trasferimento di know-how relativo alla configurazione di alcuni aspetti della soluzione con il fine di garantire una maggiore autonomia alle strutture di supporto/utenti coinvolti nella normale conduzione delle attività. Il Piano includerà inoltre un calendario per lo svolgimento di successivi approfondimenti o affiancamenti al personale.

Le attività appena descritte afferiscono al servizio previsto dall'Accordo Quadro "Conduzione Applicativa - Servizi di gestione Applicativi e Base Dati".

8.2.5 Gestione a regime

In seguito al collaudo e dispiegamento delle soluzioni, il Fornitore dovrà garantire fino al termine del contratto tutte le attività e servizi necessari ad assicurare il corretto funzionamento della soluzione, nel rispetto dei livelli di servizio descritti nel Capitolo 9.

In particolare, le attività necessarie a garantire il corretto funzionamento della soluzione di infrastruttura applicativa dovranno essere erogate dai gruppi di lavoro che il Fornitore metterà a disposizione per i servizi di:

- Gestione della domanda e Supporto per la pianificazione delle evoluzioni dei servizi: in particolare per quanto riguarda le attività necessarie a monitorare e garantire nel tempo l'allineamento fra le esigenze delle Aziende Sanitarie e l'evoluzione dei servizi stessi;
- Gestione operativa delle installazioni: per quanto riguarda le attività di assistenza e gestione di servizi applicativi e dell'infrastruttura connessa all'esercizio della soluzione;
- Supporto e Manutenzione dei servizi della soluzione: per quanto riguarda le attività di manutenzione di servizi applicativi esistenti e servizi di supporto connessi;
- Assistenza e supporto applicativo: per quanto riguarda le attività di assistenza specialistica di servizi applicativi, Help Desk di II° Livello;
- Delivery della soluzione: per le attività necessarie a far evolvere le soluzioni in esercizio nelle Aziende Sanitarie (ad es. effettuare i rilasci delle versioni della soluzione contenenti migliorie ed evoluzioni).
  Resta inteso che durante la fase di esercizio e dunque per tutta la durata del contratto il Fornitore dovrà garantire i servizi necessari ad assicurare il corretto funzionamento della soluzione, nel rispetto degli opportuni Livelli di servizio come descritto nel Capitolo 9.

Tutte le attività previste a seguito dell'avviamento delle soluzioni per per i diversi ES afferiscono ai servizi previsti dall'Accordo Quadro in ambito manutentivo: "*Manutenzione Adeguativa e Manutenzione Correttiva (MAD e MAC)", che* dovrà essere attivato al termine del periodo di garanzia full risk previsto per i 12 mesi successivi al collaudo applicativo fino a fine contratto, *e di "Conduzione Applicativa - Servizi di gestione applicativi e Base Dati", "Servizi Infrastrutturali - Servizio di conduzione tecnica", che* dovranno essere attivati dal collaudo degli applicativi fino a fine contratto.

8.3 Exit strategy

Nella presente sezione sono descritte le attività e procedure richieste al Fornitore nella fase finale del rapporto contrattuale, con l'obiettivo di facilitare la transizione al personale delle Aziende Sanitarie nelle specifiche aree di competenze, garantendo la continuità operativa per gli utenti dei servizi erogati. Al fine di garantire la corretta pianificazione di questa fase, dovrà essere redatto dal fornitore ed approvato dalle Aziende Sanitarie il Piano di Trasferimento, adattabile in base alle esigenze e richieste delle Aziende che potrebbero occorrere durante la fase di trasferimento. Alla scadenza del contratto, il Fornitore proponente fornirà l'assistenza necessaria per trasferire la gestione dei servizi al Committente o a una terza parte identificata dal Committente per un periodo di almeno cinque (5) mesi prima della conclusione del contratto.

La fase di *Exit Management*, oltre a quanto detto, prevede i seguenti aspetti:

- Fornitura del servizio e delle modalità per garantire la continuità durante il trasferimento.
- Gestione del processo di trasferimento, inclusi ruoli, responsabilità, autorizzazioni e risorse da assegnare.
- Diritti di proprietà intellettuale: accordi necessari, licenze, codice (se applicabile), ecc.
- Due diligence: definizione della documentazione e dei contenuti da trasferire al nuovo Fornitore subentrante, nonché definizione di altre obbligazioni e penalità previste.
- Contratti e licenze.

- Sicurezza.
- Piano di comunicazione.

In particolare, in base ai contenuti e alle caratteristiche dell'attività di *Exit Management*, il Fornitore proponente deve impegnarsi durante la fase finale del contratto a soddisfare i seguenti requisiti generali:

- Il passaggio delle consegne non deve generare alcun impatto o interruzione nei servizi erogati.
- Non devono verificarsi diminuzioni nei livelli di servizio attribuibili direttamente al processo di transizione delle responsabilità e all'assistenza del personale del fornitore a quello subentrante.
- Dall'ottica dell'utente finale, non devono esserci cambiamenti significativi imputabili al passaggio delle consegne che possano influire sulle attività operative.

La proposta di una adeguata strategia di Exit Management sarà oggetto di valutazione tecnica approfondita.

Di seguito si riportano gli elementi chiave e alcune caratteristiche qualificanti dell'attività di *Exit Management* che il Fornitore dovrà progettare e gestire insieme al Committente:

- **Piano di Trasferimento:** tale Piano dovrà essere redatto dal Fornitore e sarà oggetto di approvazione da parte delle Aziende Sanitarie. Il Piano dovrà contenere le attività di affiancamento e rilascio, riportando in maniera precisa i requisiti, vincoli e termini stabiliti nei documenti contrattuali.
- **Responsabilità:** durante il periodo di affiancamento e migrazione alla fine del contratto, la responsabilità del servizio resta sotto la gestione del Fornitore fino alla data di scadenza contrattuale stabilita.
- **Governo del processo:** il Fornitore assicura tutte le attività finalizzate a coordinare e verificare la corretta ed efficace esecuzione delle attività di Affiancamento e Rilascio nel rispetto dei termini concordati nonché la coerenza con i requisiti, i vincoli ed i termini stabiliti nei documenti contrattuali. L'attività sarà svolta da una figura unica, individuata nel Project Manager, responsabile del coordinamento di tutte le attività e di interfacciarsi con il Committente e, eventualmente, con il Fornitore subentrante.
- **Continuità dei servizi:** al fine di garantire al Committente il mantenimento dei livelli di servizio richiesti da parte del subentrante, nel Piano di Transizione sono previste fasi di verifica e validazione del trasferimento del know-how e del rilascio della documentazione. Durante il processo di trasferimento delle competenze, è previsto un periodo adeguato in cui le risorse del fornitore subentrante lavoreranno a stretto contatto con le attività operative in corso del fornitore uscente.
- **Risorse professionali:** un gruppo di risorse del Fornitore appositamente designato affiancherà le risorse del Committente e/o del Fornitore subentrante per il trasferimento delle conoscenze sui servizi e sulle relative attività di gestione; il team sarà composto da personale già impegnato nell'erogazione dei servizi.

8.4 Gestione della Fornitura

L'impianto contrattuale con il Fornitore, individuato tramite procedura di gara, deve prevedere un contratto esecutivo come riportato nel paragrafo 2.5.

8.4.1 Governo della Fornitura

In questa sede non verranno imposti vincoli sull'organizzazione che il Fornitore deve dare alle proprie risorse, ma solo per quanto riguarda Competenze/Ruoli chiave. A questo proposito, è onere del Proponente fornire evidenza della qualità dell'organizzazione e delle figure proposte.

Allo stesso modo, è necessaria l'adozione, documentata, di un modello di governo secondo metodologie di riferimento quali il Framework PMBoK (Project Management Body of Knowledge del Project Management Institute), PRINCE/PRINCE2 (PRojects IN Controlled Environments), o analogo framework riconosciuto di project management per la pianificazione e successiva gestione di ogni fase dell'iniziativa. Coerentemente con la metodologia scelta, è poi opportuno effettuare, fin dall'inizio della Fornitura, un tailoring sulla base delle specifiche esigenze e del contesto organizzativo in essere.

È, inoltre, necessario l'utilizzo, documentato, del Framework ITIL (Information Technology Infrastructure Library), COBIT (Control Objectives for Information and related Technology), CMMI (Capability Maturity Model Integration) o analogo framework di gestione dei processi per l'implementazione dei processi di erogazione dei servizi richiesti. Il Fornitore è tenuto a documentare come ha adottato e intende implementare una metodologia di lavoro strutturata per la gestione operativa dei servizi applicativi e dei servizi professionali richiesti.

Gli ES si riservano di valutare e segnalare incompatibilità del personale predisposto dal Proponente per l'erogazione della Fornitura e richiederne la sostituzione, con istanza insindacabile.
In caso di variazione al gruppo di lavoro, il Proponente deve assicurare alle nuove risorse un periodo di affiancamento come da Livelli di servizio, senza ulteriori oneri.

8.4.2 Gestione del contratto con il Fornitore e relative tempistiche

I momenti di controllo e verifica dell'andamento della fornitura sono costanti per tutta la durata del contratto esecutivo e garantiscono una visibilità completa e dettagliata dell'avanzamento delle attività. Le attività di verifica e controllo riguardano:

- verifica dell'andamento operativo della fornitura (SAL Operativo);
- verifica dell'andamento economico e generale del contratto (SAL Economico-Generale).

Il dettaglio è riportato nella tabella che segue:

Dettagli su attività di verifica e controllo					
Attività di verifica	**Oggetto**	**Finalità**	**Attori**	**Frequenza**	**Output**
SAL OPERATIVO	Uno o più Servizi/attività	Monitoraggio attività operative, controllo costi e attestazione di consegna dei rilasci, controllo della qualità della fornitura e del rispetto degli SLA definiti	Referente nominato dall' ES e referente del Fornitore	Mensile o su richiesta dell'Ente.	Verbale di SAL
SAL ECONOMICO - GENERALE	Intero contratto esecutivo	Verifica costi, consumi e andamento generale del contratto	Referente nominato dall'ES e referente del Fornitore	Su richiesta dell'Ente.	Verbale di SAL

8.4.3 Ruoli di Governo

Di seguito sono descritti i principali attori coinvolti nel governo della Fornitura.

Responsabile del Contratto del Fornitore: il Fornitore deve individuare un proprio Responsabile del Contratto che costituirà il suo punto di riferimento nei confronti della Regione per tutte le necessità di governo del contratto.
Comitato di Direzione: Le Aziende Sanitarie/Ospedaliere committenti avranno facoltà di definire un Comitato di Direzione per esercitare il controllo sull'attuazione generale del Servizio.
Il Comitato di Direzione deve esercitare il controllo strategico sul Servizio ed essere incaricato della valutazione dello stato di avanzamento complessivo.

8.4.4 Principali processi di Governo

Di seguito vengono descritti i principali processi di Governo che regolamentano la gestione dei rapporti fra ES e Fornitore. Gli organismi di Governo devono gestire i seguenti processi principali:

- Monitoraggio e controllo della fornitura
- Segnalazione delle anomalie rispetto ai livelli di servizio concordati e determinazione delle penali;
- Gestione dell'erogazione della fornitura;
- Processi di audit.

8.4.5 Gestione operativa della Fornitura

Le funzioni di erogazione dei servizi agiscono sotto il coordinamento dei ruoli di governo. Hanno un'autonomia organizzativa e operativa, ma sono al tempo stesso allineate tra loro e alle funzioni di governo

da un *framework* di obiettivi coerente. Le parti che seguono hanno l'obiettivo di specificare ruoli e responsabilità di una figura che si ritiene sia chiave in termini di interfaccia operativa tra fornitore e l'ente Regionale. Di seguito si descrivono le competenze del ***Project Manager*** di cantiere che il Fornitore deve indicare quale referente operativo per la realizzazione di quanto previsto contrattualmente.

Si precisa che il *Project Manager* di cantiere deve essere il riferimento di più alto livello per la gestione del progetto nel suo complesso e per la risoluzione delle potenziali problematiche che potrebbero presentarsi.

Al fine di garantire un efficace coordinamento e monitoraggio delle attività effettuate, il singolo *Project Manager* di cantiere deve garantire un supporto continuativo e dedicato; pertanto, il Fornitore deve considerare il suo impegno nel periodo compreso tra la data di avvio del progetto e la conclusione.
Relativamente alle caratteristiche richieste per tale tipologia di profilo (*Project Manager*) si prega di far riferimento a quelle esplicitate all'Appendice 1A ("Profili Professionali") Al Capitolato Tecnico Speciale dell'Accordo Quadro CONSIP "Servizi Applicativi in ambito "Sanità digitale - Sistemi informativi sanitari e servizi al cittadino" per le Pubbliche Amministrazioni del SSN.

8.5 Manutenzione, assistenza, conduzione applicativa e rendicontazione

8.5.1 Manutenzione

Il Fornitore deve garantire la manutenzione sui sistemi e applicativi preposti all'erogazione della fornitura come:

Manutenzione correttiva ed adeguativa (MAC e MAD): comprende tutti gli interventi volti ad indagare e rimuovere le cause e gli effetti di eventuali malfunzionamenti dei sistemi e applicativi preposti all'erogazione delle soluzioni oggetto della presente fornitura (ad esempio interfacce utente, base dati,ecc...) che determinano un comportamento del sistema difforme da quello definito in specifica, anche in termini di prestazioni, assicurando il ripristino dell'operatività. Sono parte di tali interventi:

o La presa in carico delle segnalazioni di malfunzionamento, la loro gestione e risoluzione;

oI contributi di competenza sistemistica e specialistica necessari alla corretta soluzione del malfunzionamento;

o Il ripristino di basi dati danneggiate dagli errori;

o Il ripristino da malfunzionamenti del software;

o La modifica della documentazione per il mantenimento della coerenza con quanto erogato.

o Manutenzione funzionale all'adeguamento del sistema alle variazioni sia tecnologiche (es: aggiornamento dei sistemi operativi o dei browser) che organizzative/normative (sono incluse tutti gli adeguamenti derivanti da variazioni normative o direttive di carattere europeo, nazionale o regionale che dovessero insorgere durante il periodo di validità del contratto; migliorie di carattere ordinario, adeguamento delle tabelle di configurazione dei database, della configurazione di report/stampe/maschere, etc…).

La manutenzione correttiva ed adeguativa sono comprese nella Fornitura. Il servizio di Manutenzione Adeguativa dovrà essere attivato al termine del periodo di garanzia full risk previsto per i 12 mesi successivi al collaudo applicativo fino a fine contratto.

Manutenzione evolutiva (MEV): gli interventi di evoluzione delle funzionalità e delle componenti dell'architettura applicativa e gli interventi atti ad introdurre nel sistema corrente nuove funzionalità, volte a migliorare il livello di interoperabilità sanitaria. Il Fornitore sarà tenuto a rispondere alla richiesta di intervento proponendo un progetto di lavoro e la stima dell'impegno necessario, che saranno oggetto di validazione da parte dell'ente Regionale, che si riserva la facoltà di richiederne l'effettiva attivazione solo dopo aver visionato e valutato la risposta tecnica / economica del Fornitore.

8.5.2 Assistenza

Il Fornitore deve garantire assistenza e supporto all'utenza mediante un servizio di help desk di II livello. Per le chiamate inerenti alla segnalazione di guasti e malfunzionamenti o alle richieste di assistenza di qualsiasi genere, deve essere definito un riferimento unico e indistinto per le varie componenti software del sistema. Tale servizio viene attivato:

- Dal servizio helpdesk di I°e II° livello del Fornitore, a fronte di richieste e segnalazioni di guasto, da parte degli utenti, che non possono essere risolte dallo stesso;
- Da richieste del personale ICT dell' Aziende Sanitarie per problematiche afferenti ai sistemi comprese le integrazioni;
- Da richieste del personale aziendale referente per ambito di attività;
- Da allarmi del sistema di monitoraggio aziendale.

Il Fornitore deve mettere a disposizione idonee procedure operative di verifica sui sistemi/servizi oggetto di fornitura, nonché raccogliere le casistiche di segnalazione/soluzione in un apposito sistema di Knowledge Base condiviso tra la Regione e le Aziende Sanitarie e destinato alla esecuzione semplice e rapida di operazioni basiche al I° Livello competente. Il Fornitore dovrà mettere a disposizione un sistema di Trouble Ticketing (TTS) atto a gestire le richieste di assistenza e i relativi ticket per monitorarne i tempi di risposta del servizio di assistenza. Tale sistema TTS dovrà essere strutturato per ripartire, a seconda della struttura di provenienza, le richieste pervenute dalle Aziende Sanitarie o da PuntoZero s.c.a.r.l.

Nell'ottica di garantire la fruibilità della soluzione oggetto di fornitura, l'assistenza di II° livello richiesta in generale deve:

• prendere in carico le segnalazioni ricevute da parte di operatori, da parte del sistema di helpdesk di I° livello o dal sistema di monitoraggio aziendale;

• risolvere le segnalazioni in merito a problematiche riscontrate nel rispetto dei livelli di servizio contrattuali;

• gestire le segnalazioni e le comunicazioni agli interlocutori indicati dalla Regione in caso di anomalie/incidenti;

• supportare, ove necessario, PuntoZero e le Aziende Sanitarie nell'utilizzo della soluzione oggetto di fornitura;

• predisporre e realizzare tutti gli interventi di supporto nelle fasi di avviamento di una nuova funzionalità o di una personalizzazione di funzionalità già in esercizio;

• eseguire estrazioni estemporanee di dati.

Il servizio richiesto ha la responsabilità di affrontare e risolvere i problemi segnalati; in particolare, deve garantire:

• accettazione e registrazione o presa in carico della richiesta di assistenza ricevuta tramite i canali definiti con assegnazione del livello di urgenza;

• analisi del problema e risoluzione;

• comunicazione tempestiva ed efficace con i livelli di assistenza o direttamente con gli interlocutori interessati (es tecnici PuntoZero, personale ICT, ecc);

• chiusura della richiesta di assistenza ed eventuale verifica con gli interlocutori interessati (es tecnici PuntoZero, personale ICT, ecc) in caso di segnalazioni dirette;

• fornire supporto per l'affiancamento a primi gruppi di utenti ed eventuale partecipazione per la preparazione ed erogazione degli interventi formativi mirati all'utilizzo delle applicazioni in caso di avviamento di nuove funzionalità o di nuovi servizi.

In caso di problemi che richiedano modifiche di prodotto dovranno essere fornite, ove possibile, soluzioni temporanee (workaround).

L'assistenza del Fornitore deve inoltre garantire un costante e continuo allineamento delle strutture competenti della Regione e dell'Azienda Sanitaria durante la risoluzione delle problematiche più complesse o nei casi in cui siano richiesti tempi più lunghi di lavorazione per la risoluzione e la chiusura del problema segnalato (sempre nel rispetto dei livelli di servizio contrattuali).

Per una corretta erogazione dell'assistenza è necessario effettuare una classificazione dei possibili malfunzionamenti in modo da attribuire correttamente l'urgenza da associare ad ogni segnalazione.

All'interno dei servizi di conduzione applicativa e infrastrutturale previsti nella fornitura, al Fornitore è richiesta l'assistenza dalle 8:00 alle 20:00 (giorni feriali, incluso il sabato) tramite help desk remoto. Per l'extra-orario (oltre le ore 20,00 – dal lunedì al venerdì e oltre le 14.00 del sabato) è richiesta la reperibilità telefonica, prevista all'interno dei servizi di gestione operativa e remunerata come previsto nell' ALLEGATO

2A - CAPITOLATO TECNICO SPECIALE - LOTTI APPLICATIVI 1-2-3-4 «Sanità Digitale - Sistemi Informativi Sanitari e servizi al Cittadino» capitolo 8.2.

Le modalità di dettaglio dovranno essere concordate con l'Amministrazione nella fase di progettazione esecutiva della fornitura.

8.5.3 Conduzione applicativa

Al Fornitore è richiesto il servizio di "Conduzione Applicativa", secondo quanto descritto nel Capitolato Tecnico Speciale dell'Accordo Quadro CONSIP "Servizi Applicativi in ambito "Sanità digitale - Sistemi informativi sanitari e servizi al cittadino" per le Pubbliche Amministrazioni del SSN, le attività del servizio trovano collocazione rispetto alla maggior parte delle fasi previste. Sono parte integrante del servizio le principali attività riportate nel seguito:

- Supporto alla predisposizione dell'ambiente di esercizio, e quanto necessario a consentire l'inizio delle attività da parte degli utenti;
- Presa in carico e messa in esercizio delle architetture software
- Gestione delle applicazioni, loro base dati e data services
- Presa in carico di nuove funzionalità in esercizio e attività di parametrizzazione specifiche su procedure, parametri e tabelle, ecc.

8.5.4 Conduzione tecnica

Al Fornitore è richiesto il servizio di "Conduzione Tecnica", secondo quanto descritto nel Capitolato Tecnico Speciale dell'Accordo Quadro CONSIP "Servizi Applicativi in ambito "Sanità digitale - Sistemi informativi sanitari e servizi al cittadino" per le Pubbliche Amministrazioni del SSN, le attività del servizio trovano collocazione rispetto alla maggior parte delle fasi previste. Sono parte integrante del servizio:

- Presa in carico e messa in esercizio delle architetture hardware
- Supporto nella messa in esercizio delle applicazioni e presa in carico delle stesse;
- Help Desk 2° livello di tipo tecnico

8.5.5 Rendicontazione

La Fornitura deve fornire un ambiente di rendicontazione in grado di presentare, tramite cruscotti informativi e rapporti di dettaglio, i valori aggiornati e su base storica di una serie di indicatori di erogazione della Fornitura.
I cruscotti e i rapporti, specifici nei contenuti offerti in funzione del fruitore cui sono indirizzati, devono fornire un resoconto sul funzionamento della soluzione oggetto di fornitura, sia in termini di volumi di transizioni avvenute, che volumi di transizioni gestite dai singoli laboratori, ed essere prodotti

dinamicamente sulla base di parametri di indagine (ad es. periodo di osservazione, tipologia documentale, analisi realizzate ecc.) definiti dall'operatore. Devono in particolare essere resi disponibili specifici rapporti finalizzati al calcolo dei costi della Fornitura, sia per il controllo dei costi da parte delle Aziende Sanitarie, sia per il monitoraggio complessivo da parte delle autorità istituzionali.
L'ambiente di rendicontazione deve permetterne la consultazione, l'archiviazione e il download su postazione di lavoro dei rapporti prodotti in formati standard o di mercato ad alta diffusione (quali ad esempio PDF, Excel, Libreoffice, ecc.).
Infine, come già precedentemente descritto, il Fornitore deve mettere a disposizione un sistema professionale di performance monitoring per l'intera durata contrattuale (sia in sede di collaudo che in sede di erogazione a regime) finalizzato alla misurazione end-to-end del numero di richieste gestite e dei tempi di risposta del sistema.
La definizione dei contenuti dei cruscotti e dei rapporti deve essere prodotta dal Fornitore secondo uno schema condiviso e validato dal Comitato di Direzione.

9 LIVELLI DI SERVIZIO E PENALI

In questa parte del documento si definiscono gli indicatori atti a descrivere i Livelli di qualità dei Servizi (LdS), che devono essere applicati alle forniture oggetto dell'Appalto, le relative modalità di rilevazione, i Livelli di Servizio minimi richiesti e il periodo di misurazione su cui calcolare il valore dell'indicatore.

Il Fornitore, durante l'intera durata dell'incarico, **deve periodicamente produrre e consegnare specifici rapporti di dettaglio** che verranno utilizzati per la valutazione del rispetto dei Livelli di Servizio costruiti secondo formati e contenuti coerenti con la tipologia dell'indicatore in esame e con periodicità congruente con il relativo periodo di riferimento. La struttura dei rapporti deve essere prodotta dal Fornitore secondo uno schema condiviso e approvato dal Committente. Per alcuni Livelli di Servizio, esplicitamente indicati, le informazioni elementari raccolte dal Fornitore per il calcolo degli stessi devono essere registrate, *su base giornaliera*, in specifici *file* in formato concordato con le aziende tra cui doc, csv, excel, pdf secondo le necessità che devono:

- possedere un identificativo progressivo;
- essere marcati temporalmente.

Si precisa che tali file devono essere prodotti su un template condiviso e approvato dal Committente, ed essere utilizzati per verificare la correttezza dei report dei Livelli di Servizio.

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

I Livelli di Servizio che trovano applicazione in questa gara sono relativi alla richiesta di fornitura e sono definiti a partire dall'allegato 2 del Capitolato Tecnico Speciale dell'AQ "Servizi Applicativi in ambito "Sanità digitale - Sistemi informativi sanitari e servizi al cittadino" per le Pubbliche Amministrazioni del SSN, suddivisi nelle seguenti macro-categorie:

1. Governo della fornitura;
2. Servizi realizzativi;
3. Manutenzione Correttiva (MAC) e Adeguativa (MAD);
4. Assistenza ed Help-desk di I° e II° livello.
5. Conduzione Applicativa;
6. Conduzione Tecnica;

Relativamente alle tipologie di azione contrattuale per singolo Livello di Servizio e alla loro descrizione di dettaglio si prega di far riferimento a quelle esplicitate all' Appendice 2 ("Livelli di Servizio") al Capitolato Tecnico Speciale dell'Accordo Quadro CONSIP Servizi Applicativi in ambito "Sanità digitale - Sistemi informativi sanitari e servizi al cittadino" per le Pubbliche Amministrazioni del SSN. Nello specifico viene definita la matrice di corrispondenza tra gli Indicatori di Qualità validi per l'intera fornitura e le azioni contrattuali previste nel caso di non rispetto dei valori di soglia, ovvero rilievo, quota sospesa e penale.

Si precisa che qualora il Fornitore abbia dichiarato nella propria Offerta Tecnica il miglioramento dei valori di soglia rispetto a quanto indicato nel presente documento, gli scostamenti al fine dell'applicazione delle penali saranno calcolati rispetto ai valori soglia dichiarati nell'Offerta Tecnica.

Ciascun Livello di Servizio riporta le modalità di applicazione delle sanzioni in caso di scostamenti rispetto alla soglia definita. Rimarrà facoltà del Committente l'applicazione di penali di entità minore a quelle previste, sulla base di valutazioni inerenti al grado di responsabilità del Fornitore nel mancato rispetto del Livello di Servizio.

9.1 Governo della Fornitura

Di seguito vengono presentati gli indicatori per valutare gli aspetti rilevanti per tutti i servizi inclusi nel Contratto Esecutivo, definiti dall'AQ (Accordo Quadro):

- RSER: Impegni rispettati nell'offerta tecnica;
- PFI: Personale inadeguato;
- TIP: Tempestività nell'inserimento di personale;
- RSCT: Rispetto delle scadenze contrattuali;
- MAPP: Mancata Approvazione di un Artefatto della Fornitura;
- VQF: Valutazione Qualità della Fornitura;
- RLFN: Rilievi sulla fornitura;

- MIDG: Monitoraggio degli indicatori di digitalizzazione;
- TAI: Tempo di Attivazione degli Interventi;
- INPF: Indisponibilità del Portale di Fornitura;
- ATPF: Mancata Attivazione del Portale di Fornitura.

Per ulteriori informazioni specifiche su ciascun indicatore, si prega di fare riferimento all'Appendice 2 ("Livelli di Servizio") nel Capitolato Tecnico Speciale dell'Accordo Quadro CONSIP "Servizi Applicativi in ambito "SANITA' DIGITALE - Sistemi Informativi Sanitari e servizi al Cittadino" per le Pubbliche Amministrazioni del SSN. In particolare, fare riferimento al capitolo 4.1 "Governo della fornitura".

Oltre agli indicatori di qualità definiti nel Capitolato Tecnico Speciale, sarà anche monitorato l'indicatore di Turnover.

Codifica del LdS	**ORG-LdS01 – *Turnover***
Aspetto da valutare	Misura del numero di risorse del Fornitore sostituite
Unità di misura	Percentuale
Fonte dati	Consuntivo Attività (Rendiconto risorse)
Periodo di riferimento	Anno
Frequenza di misurazione	Annuale
Dati da rilevare	N = numero di risorse sostituite nel periodo di riferimento.
Regole di campionamento	Nessuna
Formula	LdS = N
Regole di arrotondamento	Nessuna
Valore di soglia (Risultati attesi)	LdS ≤ 1
Azioni contrattuali	Il Livello di servizio si applica sia nel caso di sostituzione dovuta ad una decisione del Fornitore (poiché è importante garantire la stabilità e la continuità operativa del personale impiegato) sia al caso di sostituzione motivatamente richiesta da parte dell'Azienda Sanitaria (che può valutare le risorse messe a disposizione dal Fornitore)

9.2 Servizi realizzativi

Di seguito vengono descritti gli indicatori di qualità da applicare ai Servizi Realizzativi per la produzione dei software, come definiti nell'AQ (Accordo Quadro):

- RSPL: Rispetto del Piano di lavoro di obiettivo;
- GSCO: Giorni di sospensione del collaudo;
- DAES: Difettosità in avvio in esercizio;
- CTFU: Copertura test funzionali;
- RIUSO: Riuso di componenti;
- TRCG: Tempestività di Ripristino dell'Operatività in collaudo ed in garanzia;
- VISS: Violazioni degli standard di sviluppo;
- TROR: Totale Rilievi Obiettivo Realizzativo.

Per ulteriori informazioni specifiche su ciascun indicatore, si prega di fare riferimento all'Appendice 2 ("Livelli di Servizio") nel Capitolato Tecnico Speciale dell'Accordo Quadro CONSIP " SANITA' DIGITALE - Sistemi Informativi Sanitari e servizi al Cittadino" per le Pubbliche Amministrazioni del SSN. In particolare, fare riferimento al capitolo 4.2 "Servizi Realizzativi".

9.2.1 Collaudo

Durante il periodo di collaudo, come definito nel Capitolo 8.3 dell'Allegato 2A del Capitolato Tecnico Speciale Lotti dell'AQ, l'obiettivo è verificare e convalidare il sistema rilasciato. È considerata normale una residua presenza di difetti rispetto alle attività di test effettuate dal fornitore. Questa difettosità residua può includere malfunzionamenti non bloccanti e test negativi eseguiti in modi diversi da quanto dichiarato positivamente dal fornitore. Al contrario, i malfunzionamenti bloccanti sono disciplinati dall'indicatore successivo, DFCC - Difettosità in collaudo. Tutti i malfunzionamenti e le non conformità devono essere risolti per l'accettazione del software.

Il fornitore è tenuto a fornire supporto e garantire la tempestiva correzione degli errori nel software e nella documentazione entro i tempi previsti dal TRCG - Tempestività di Ripristino dell'Operatività in collaudo ed in garanzia. Si precisa che sono considerate bloccanti le non conformità relative a:

- Sicurezza e protezione dei dati: per tutti gli interventi realizzativi, inclusi gli interventi correttivi;

- Manutenibilità, interoperabilità, efficienza prestazionale, affidabilità: per tutti gli interventi che realizzano servizi IT in Cloud e migrazione di applicativi in Cloud;

- Manutenibilità e affidabilità: per tutti gli interventi realizzativi su applicazioni di classe A;

- Usabilità e portabilità: per tutti gli interventi che realizzano o modificano servizi esposti all'esterno (siti, portali, app mobili).

Nei casi diversi, fermo restando che tutte le non conformità devono essere risolte per l'accettazione del software, saranno considerate non bloccanti.

Di seguito sono descritti gli indicatori per la fase di collaudo definiti dall'AQ:

- DFCC: Difettosità in collaudo;
- MDTE: Miglioramento del Debito Tecnico (moduli preesistenti);
- QNFU: Qualità Non Funzionale.

Per ulteriori informazioni specifiche su ciascun indicatore, si fare riferimento all'Appendice 2 ("Livelli di Servizio") nel Capitolato Tecnico Speciale dell'Accordo Quadro CONSIP "S SANITA' DIGITALE - Sistemi Informativi Sanitari e servizi al Cittadino" per le Pubbliche Amministrazioni del SSN. In particolare, fare riferimento al capitolo 4.2.9 "Collaudo".

9.3 Manutenzione Correttiva (MAC) e Adeguativa (MAD)

Di seguito sono descritti gli indicatori di qualità applicabili al Servizio di Manutenzione Correttiva e Adeguativa definiti da AQ:

- TROI: Tempestività di Ripristino dell'Operatività in esercizio;
- CSR: Interventi di manutenzione correttiva recidivi;
- RMCO: Rilievi di Manutenzione Correttiva.

Per ulteriori informazioni specifiche su ciascun indicatore, si prega di fare riferimento all'Appendice 2 ("Livelli di Servizio") nel Capitolato Tecnico Speciale dell'Accordo Quadro CONSIP "Servizi Applicativi in ambito " SANITA' DIGITALE - Sistemi Informativi Sanitari e servizi al Cittadino" per le Pubbliche Amministrazioni del SSN. In particolare, fare riferimento al capitolo 4.3 "Manutenzione Correttiva (MAC) e Adeguativa (MAD)".

Oltre agli indicatori di qualità definiti nel Capitolato Tecnico Speciale, si prevede anche il monitoraggio dell'indicatore relativo alla Gestione del backlog.

Codifica del LdS	**ASSI-LdS01 - Gestione del *backlog***
Aspetto da valutare	Controllo del completamento della risoluzione dei *ticket* inevasi nelle tempistiche previste per tutte le categorie di urgenza
Unità di misura	Percentuale
Fonte dati	Sistema di tracciatura e/o monitoraggio
Periodo di riferimento	Mese solare precedente la rilevazione
Frequenza di misurazione	Mensile
Dati da rilevare	NTR_{15} = numero di *ticket* non risolti nelle tempistiche previste e risolti entro 15 giorni lavorativi. NTR_{30} = numero di *ticket* non risolti nelle tempistiche previste e risolti entro 30 giorni lavorativi. NToff = numero totale di *ticket* non risolti nelle tempistiche previste risolti nel periodo di riferimento o ancora in carico al Fornitore.
Regole di campionamento	Nessuna
Formula	LdS_{15} = (trasformato in %, ad es. 0,855 corrisponde a 85,5%) LdS_{30} = (trasformato in %, ad es. 0,855 corrisponde a 85,5%)
Regole di arrotondamento	Nessuna
Valore di soglia (Risultati attesi)	$LdS_{15} \geq 99{,}00\%$ $LdS_{30} = 100{,}00\%$
Azioni contrattuali	Applicazione di una penale pari a 250 € al primo scostamento al di sotto della soglia e per ogni ulteriore scostamento pari all'1%. Penali applicate per singolo livello di servizio. Le penali applicate sono cumulabili. Sono esclusi dal conteggio i *ticket* in stato sospeso per attività in corso presso livelli di assistenza esterni o non chiusi per indisponibilità degli utenti. Per il presente LdS non saranno applicate penali nei primi 4 mesi decorrenti l'avvio della fase di gestione a regime della Fornitura per la singola Azienda Sanitaria.

9.4 Conduzione applicativa

I seguenti indicatori si applicano a tutti i servizi di gestione. Nel caso di attivazione di servizi separati, i livelli di servizio vengono rilevati e calcolati distintamente. Il fornitore, per i servizi erogati presso la propria sede, deve mettere a disposizione dell'Amministrazione strumenti per la verifica della capacità di gestione delle richieste e della disponibilità del servizio stesso.

- DSGP – Disponibilità dei servizi di gestione del portafoglio applicativo;
- RSCA – Rispetto di una scadenza dei servizi di gestione del Portafoglio;
- TRRA – Tempestività di risoluzione delle richieste di assistenza;
- RSGT – Rilievi sui servizi di gestione del Portafoglio Applicativo;
- UMI - Utilizzo Medio dell'Infrastruttura;

Relativamente alle informazioni aggiuntive per singolo indicatore, si prega di far riferimento a quelle esplicitate all' Appendice 2 ("Livelli di Servizio") al Capitolato Tecnico Speciale dell'Accordo Quadro CONSIP "Servizi Applicativi in ambito "SANITA' DIGITALE - Sistemi Informativi Sanitari e servizi al Cittadino" Per Le Pubbliche Amministrazioni del SSN", nello specifico al capitolo 4.4. "Conduzione Applicativa".

Per il Livello di Servizio "TRRA", si **propone a livello esemplificativo** il seguente modello da adeguarsi ai livelli di criticità dei ticket che saranno concordati e definiti con le singole Aziende Sanitarie in fase di stipula del contratto.

Codifica del LdS	**TRRA**
Titolo del LdS	**Tempestività di risoluzione delle richieste di assistenza**
Aspetto da valutare	Misura il rispetto delle tempistiche previste per la risoluzione dei *ticket* in funzione della categoria di urgenza
Unità di misura	Percentuale
Fonte dati	Comunicazioni, Contratto Esecutivo, Piano di lavoro, strumento di tracciatura
Periodo di riferimento	Mese solare precedente la rilevazione
Frequenza di misurazione	Mensile

Dati da rilevare	NrOK = numero di *ticket* per malfunzionamento risolti nelle tempistiche previste per ogni categoria di urgenza registrati dal sistema di *ticketing* nel periodo di riferimento. NrT = numero di *ticket* per malfunzionamento risolti per ogni categoria di urgenza registrati dal sistema di *ticketing* nel periodo di riferimento.
Formula	(trasformato in %, ad es. 0,855 corrisponde a 85,5%)
Regole di arrotondamento	Nessuna
Valore di soglia	**Esempio "Urgenza Critica" (Categoria 1)**: LdS = 100% **Esempio "Urgenza Alta" (Categoria 2)**: LdS ≥ 95% **Esempio "Urgenza Media" (Categoria 3)**: LdS ≥ 90% **Esempio "Urgenza Bassa" (Categoria 4)**: LdS ≥ 90%[2] Tempistiche previste per la risoluzione dei malfunzionamenti di ciascuna classe di urgenza: **Urgenza Critica (Categoria 1):** 2 ore solari **Urgenza Alta (Categoria 2):** 4 ore solari **Urgenza Media (Categoria 3):** 30 ore solari **Urgenza Bassa (Categoria 4):** 72 ore solari
Azioni contrattuali	**1 rilievo** al primo scostamento al di sotto della soglia che andrà ad incrementare l'indicatore **RSGT**

9.5 Conduzione Tecnica

Ecco gli indicatori di qualità definiti da AQ che si applicano al Servizio di Conduzione Tecnica:

- DSA: Disponibilità dei sistemi e apparati - misura la disponibilità dei sistemi e apparati necessari per la conduzione tecnica del servizio.
- EASA: Esecuzione delle attività su sistemi e apparati - misura l'esecuzione corretta delle attività sulla base dei sistemi e apparati utilizzati nella conduzione tecnica.
- TROSA: Tempestività nel ripristino dell'operatività dei sistemi e apparati - misura la tempestività con cui viene ripristinata l'operatività dei sistemi e apparati in caso di eventuali interruzioni.
- UMI - Utilizzo Medio dell'Infrastruttura;

Per l'Utilizzo Medio dell'Infrastruttura "UMI", si **propone a livello esemplificativo** il seguente modello da adeguarsi rispetto alle richieste contrattuali avanzate da PuntoZero s.c.a.r.l che saranno concordati e definiti con le singole Aziende Sanitarie in fase di stipula del contratto.

Codifica del LdS	**UMI**
Titolo del LdS	**Utilizzo Medio Infrastruttura**
Aspetto da valutare	Corretto dimensionamento delle componenti infrastrutturali proposte dal fornitore e messe a disposizione della Stazione Appaltante
Unità di misura	Percentuale
Fonte dati	Sistemi di monitoraggio dell'infrastruttura
Periodo di riferimento	Trimestre precedente la rilevazione
Frequenza di misurazione	Trimestrale
Dati da rilevare	Utilizzo medio (escluso picchi) in percentuale di ogni componente infrastrutturale (ad esclusione della banda di rete) messa a disposizione nella fascia oraria diurna 8:00-18:00
Formula	UMI(%)= ($Utilizzo\ medio\ delle\ risorse\ infrastrutturali / Capacity\ delle\ risorse\ infrastrutturali$)$*$100
Regole di arrotondamento	Nessuna
Valore di soglia	Utilizzo medio infrastruttura >= 70 % (su rilevazione trimestrale)
Azioni contrattuali	Il mancato rispetto del valore soglia sopra riportato comporta l'applicazione di una penale pari all' 0,2% (zero virgola due per mille) dell'importo contrattuale. Ad ogni ulteriore scostamento percentuale (negativo) del 5% oltre il valore soglia comporta l'applicazione di una penale pari all'0,2‰ (zero virgola due per mille) dell'importo contrattuale.

9.6 Produzione dei rapporti dei LdS

Infine, in aggiunta agli indicatori di qualità determinati dall'AQ si vuole monitorare la produzione dei rapporti di dettaglio dei Livelli di servizio erogati.

Codifica del LdS	**REP-LdS01- Produzione dei rapporti di dettaglio dei Livelli di servizio erogati**
Aspetto da valutare	Misura il tempo medio per la consegna dei rapporti di dettaglio la cui produzione è in capo al Fornitore
Unità di misura	Giorni solari
Fonte dati	Strumenti di comunicazione E-mail, lettere, verbali
Periodo di riferimento	Mese solare precedente la rilevazione
Frequenza di misurazione	Mensile
Dati da rilevare	N = numero di rapporti previsti nel periodo di riferimento. Tr_i = tempo dalla data di termine del periodo di riferimento del rapporto i-esimo e la sua data di consegna da parte del Fornitore.
Regole di campionamento	Nessuna
Formula	LdS =
Regole di arrotondamento	Nessuna
Valore di soglia (Risultati attesi)	LdS ≤ 10 giorni solari
Azioni contrattuali	Applicazione di una penale pari a 250 € al primo scostamento al di sopra della soglia e per ogni scostamento pari a 1 giorno solare.

10 GESTIONE DEI CORRISPETTIVI E VALORE DELLA FORNITURA

10.1 Organizzazione dei corrispettivi

I corrispettivi sono parametrizzati in accordo con quanto indicato nel Capitolato Tecnico Generale dell'Accordo Quadro CONSIP "Servizi Applicativi in ambito "Sanità digitale - Sistemi Informativi Sanitari e servizi al Cittadino per le Pubbliche Amministrazioni del SSN". L'Accordo Quadro prevede di determinare i corrispettivi per la soluzione partendo dai prezzi unitari relativamente a ciascuno dei servizi richiesti nel Capitolato Tecnico Speciale dell'AQ CONSIP. Si procede al calcolo della base d'asta complessiva moltiplicando i prezzi unitari suddetti per i quantitativi espressi dagli ES affidatari (USL e AO), sommata alla stima da parte dell'Amministrazioni dei Servizi Accessori (nella misura massima del 50% del valore della base d'asta totale).

I quattro ES stipuleranno successivamente il contratto con il Fornitore aggiudicatario, sulla base delle quantità e degli importi offerti.

A livello generale l'ipotesi di distribuzione dei costi prevede:

a) Oneri di progetto per l'analisi, progettazione, installazione e configurazione/parametrizzazione, integrazioni delle soluzioni, nonché collaudo della fornitura per la messa in esercizio.
b) Oneri di gestione a regime della soluzione inerenti ai costi di diffusione della soluzione, formazione e conduzione (applicativa e servizi infrastrutturali) del sistema in esercizio (es. help-desk, MAD, MAC, CT, ecc.). I corrispettivi saranno erogati a canone.

I driver di costo definiti dall'Accordo Quadro ed utili alla definizione dei valori da associare alle componenti di fornitura del presente Appalto Specifico sono riportati nella tabella che segue (Servizio di riferimento previsto dall'Accordo Quadro) che esplicita la correlazione con le singole componenti di fornitura del presente appalto specifico.

Servizio di riferimento previsto dall'Accordo Quadro	Componente di fornitura dell'Appalto Specifico	Metrica
Servizio di Sviluppo di Applicazioni Software Ex-novo- Green Field (GF)	Realizzazione, che include analisi, installazione, configurazioni ed integrazioni, e collaudo per la messa in esercizio dell'infrastruttura applicativa	GG/Team Ottimale
Servizio di Parametrizzazione e Personalizzazione di Soluzioni di terze parti/open source/riuso (PP)	Parametrizzazione e sviluppo interfacce per integrazioni Digital hub regionale (DIH)	GG/Team Ottimale
Conduzione Applicativa - Servizi di gestione Applicativi e Base Dati (GAB)	Conduzione applicativa, gestione basi dati e data services	GG/Team Ottimale
	Assistenza e formazione	GG/Team Ottimale
Servizi infrastrutturali – Conduzione Tecnica	Presa in carico e messa in esercizio delle architetture hardware e assistenza help desk II livello	GG/Team Ottimale

Manutenzione Adeguativa e Manutenzione Correttiva (MAD-MAC)	Manutenzione Adeguativa e Correttiva (fuori garanzia)	FTE/mese
Servizi accessori di gestione operativa	Servizi di conduzione applicativa e tecnica in reperibilità telefonica extra-orario	Canone
Servizi accessori licenze	Soluzioni di infrastruttura applicativa oggetto della fornitura	Corrispettivo “una tantum”

Per quanto riguarda i corrispettivi, sono previsti corrispettivi omogenei sulle quattro aziende Umbre che si divideranno in maniera uguale i costi di realizzazione e messa a regime della soluzione, al netto dei costi di licenze, suddivisi rispetto all’oggetto di fornitura. I costi di gestione a regime fino alla fine del contratto sono stati distribuiti per i quattro ES sulla base del peso dei costi di realizzazione, che tengono conto dello scorporo dei costi del middleware per la USL1 e AO Perugia.

10.2 Realizzazione e collaudo per la messa in esercizio

I corrispettivi saranno riconosciuti sulla base del raggiungimento degli obiettivi di progetto per traguardare i target PNRR (giugno 2025).

La realizzazione e l’implementazione degli applicativi di infrastruttura applicativa saranno remunerati mediante un corrispettivo così suddiviso.

-il 70% all’esito positivo del collaudo di ogni singolo applicativo oggetto di fornitura;
-il 20% all’esito della verifica di conformità dell’avvio in esercizio dell’intero sistema di infrastruttura applicativa oggetto di fornitura;
-il 10% della quota fissa, al termine della verifica di conformità della documentazione completa.

I corrispettivi seguiranno le tempistiche riportate nel GANTT allegato “AS_Infrastruttura applicativa ipotesi macro gantt”. Le suddette tempistiche potranno essere migliorate in sede di presentazione di offerta tecnica.

Inoltre, i costi tengono conto delle licenze, il cui riconoscimento del corrispettivo *una tantum* sarà al superamento del collaudo.

10. 3 Gestione a regime: Manutenzione, assistenza e gestione operativa della soluzione

Tale servizio sarà implementato tramite i seguenti servizi:

• servizi di Manutenzione Adeguativa (MAD) e Manutenzione Correttiva (MAC). Queste attività devono essere definite, in accordo con il Capitolato Tecnico Speciale dell'AQ, come modalità progettuale a canone senza oneri aggiuntivi per le aziende sanitarie.

• Servizio di Help-desk. Queste attività devono essere definite come modalità progettuale a canone senza oneri aggiuntivi per le aziende sanitarie

• Servizi Infrastrutturali di Conduzione Tecnica (CT) - Queste attività devono essere definite come modalità progettuale a canone senza oneri aggiuntivi per le aziende sanitarie.

• Servizi di Conduzione applicativa - Queste attività devono essere definite come modalità progettuale a canone senza oneri aggiuntivi per le aziende sanitarie.

I corrispettivi per i servizi sopra citati verranno riconosciuti a partire dal collaudo di tutti i servizi oggetto di fornitura fino a fine contratto. Si specifica che il servizio di manutenzione(MAD-MAC), a livello di corrispettivi, verrà riconosciuta a partire dal termine dei 12 mesi di garanzia (come anche citato nel Capitolato Generale dell'Accordo Quadro CONSIP "Servizi Applicativi in ambito "Sanità digitale - Sistemi Informativi Sanitari e servizi al Cittadino per le Pubbliche Amministrazioni del SSN") successivi al collaudo.

11 Elementi Dimensionali

Il Capitolo riassume gli elementi dimensionali della Fornitura. Tutte le quantità riportate nel presente Capitolo sono da considerarsi indicative del fabbisogno stimato dalle Aziende e rappresentano i driver di definizione del valore, predeterminato, del contratto esecutivo che ogni Azienda sottoscriverà con il fornitore.

USL UMBRIA 1			
Servizio	**Metrica**	**Prezzo maggiorato offerto in AQ**	**Totale prezzo in AS**
Servizio di Sviluppo di Applicazioni Software Ex-novo- Green Field (GF) - *rif. documento 8.2.2*	GG/team ottimale	232,04 €	112.539,40 €
Servizio di Parametrizzazione e Personalizzazione di Soluzioni di terze parti/open source/riuso (PP) - *rif. documento 8.2.2*	GG/team ottimale	211, 32 €	29.162,16 €
Servizi di licenze - *rif. documento 5.7 (somma delle voci di licenze sotto riportate)*	Corrispettivo una tantum		72.000,00 €
Licenze per MPI	*Corrispettivo una tantum*		*24.000,00 €*
Licenze per ACO	*Corrispettivo una tantum*		*12.000,00 €*
Licenze per DTS	*Corrispettivo una tantum*		*12.000,00 €*

Licenze per I&PM	*Corrispettivo una tantum*		*12.000,00 €*
Licenze per CDR	*Corrispettivo una tantum*		*12.000,00 €*
Conduzione Applicativa - Servizi di gestione Applicativi e Base Dati (GAB) - *rif. documento 8.2.4 e 8.2.5*	GG/team ottimale	192,40 €	50.024,00 €
Servizi infrastrutturali – Conduzione Tecnica - *rif. documento 8.2.5*	GG/team ottimale	207,63 €	5.606,01 €
Manutenzione Adeguativa e Manutenzione Correttiva (MAD-MAC) - *rif. documento 8.2.5*	FTE/mese	3.884,30 €	15.537,20 €
Servizi di gestione operativa	canone		15.986,72 €
Totale			**300.855,49 €**

USL UMBRIA 2			
Servizio	**Metrica**	**Prezzo maggiorato offerto in AQ**	**Totale prezzo in AS**
Servizio di Sviluppo di Applicazioni Software Ex-novo- Green Field (GF) - *rif. documento 8.2.2 e 8.2.3*	GG/team ottimale	232,04 €	182.151,40 €
Servizio di Parametrizzazione e Personalizzazione di Soluzioni di terze parti/open source/riuso (PP) - - *rif. documento 8.2.2*	GG/team ottimale	211, 32 €	29.162,16 €
Servizi di licenze - *rif. documento 5.7 (somma delle voci di licenze sotto riportate)*	Corrispettivo una tantum		97.000,00 €
Licenze per MPI	*Corrispettivo una tantum*		*24.000,00 €*
Licenze per ACO	*Corrispettivo una tantum*		*12.000,00 €*
Licenze per DTS	*Corrispettivo una tantum*		*12.000,00 €*
Licenze per I&PM	*Corrispettivo una tantum*		*12.000,00 €*
Licenze per CDR	*Corrispettivo una tantum*		*12.000,00 €*
Licenze per middleware di integrazione	*Corrispettivo una tantum*	192,40 €	*25.000,00 €*
Conduzione Applicativa - Servizi di gestione Applicativi e Base Dati (GAB) - *rif. documento 8.2.4 e 8.2.5*	GG/team ottimale	192,40 €	73.112,00 €
Servizi infrastrutturali – Conduzione Tecnica - *rif. documento 8.2.5*	GG/team ottimale	207,63 €	8.097,57 €
Manutenzione Adeguativa e Manutenzione Correttiva (MAD-MAC) - *rif. documento 8.2.5*	FTE/mese	3.884,30 €	23.305,80 €
Servizi di gestione operativa	canone		23.005,28 €

Evoluzione di Applicazioni Software Esistenti (a richiesta): *rif. documento 7.2*	GG/team ottimale	202.35 €	20.235,00 €
Totale			**456.069,21 €**

AZIENDA OSPEDALIERA DI PERUGIA			
Servizio	**Metrica**	**Prezzo maggiorato offerto in AQ**	**Totale prezzo in AS**
Servizio di Sviluppo di Applicazioni Software Ex-novo- Green Field (GF) - *rif. documento 8.2.2*	GG/team ottimale	232,04 €	112.539,40 €
Servizio di Parametrizzazione e Personalizzazione di Soluzioni di terze parti/open source/riuso (PP) - *rif. documento 8.2.2*	GG/team ottimale	211, 32 €	29.162,16 €
Servizi di licenze - *rif. documento 5.7 (somma delle voci di licenze sotto riportate)*	Corrispettivo una tantum		72.000,00 €
Licenze per MPI	*Corrispettivo una tantum*		*24.000,00 €*
Licenze per ACO	*Corrispettivo una tantum*		*12.000,00 €*
Licenze per DTS	*Corrispettivo una tantum*		*12.000,00 €*
Licenze per I&PM	*Corrispettivo una tantum*		*12.000,00 €*
Licenze per CDR	*Corrispettivo una tantum*		*12.000,00 €*
Conduzione Applicativa - Servizi di gestione Applicativi e Base Dati (GAB) - *rif. documento 8.2.4 e 8.2.5*	GG/team ottimale	192,40 €	50.024,00 €
Servizi infrastrutturali – Conduzione Tecnica - *rif. documento 8.2.5*	GG/team ottimale	207,63 €	5.606,01 €
Manutenzione Adeguativa e Manutenzione Correttiva (MAD-MAC) - *rif. documento 8.2.5*	FTE/mese	3.884,30 €	15.537,20 €
Servizi di gestione operativa	canone		15.986,72 €
Totale			**300.855,49 €**

AZIENDA OSPEDALIERA DI TERNI			
Servizio	**Metrica**	**Prezzo maggiorato offerto in AQ**	**Totale prezzo in AS**
Servizio di Sviluppo di Applicazioni Software Ex-novo- Green Field (GF) - *rif. documento 8.2.2 e 8.2.3*	GG/team ottimale	232,04 €	182.151,40 €
Servizio di Parametrizzazione e Personalizzazione di Soluzioni di terze parti/open source/riuso (PP) - *rif. documento 8.2.2*	GG/team ottimale	211, 32 €	29.162,16 €

Servizi di licenze - *rif. documento 5.7 (somma delle voci di licenze sotto riportate)*	Corrispettivo una tantum		97.000,00 €
Licenze per MPI	*Corrispettivo una tantum*		*24.000,00 €*
Licenze per ACO	*Corrispettivo una tantum*		*12.000,00 €*
Licenze per DTS	*Corrispettivo una tantum*		*12.000,00 €*
Licenze per I&PM	*Corrispettivo una tantum*		*12.000,00 €*
Licenze per CDR	*Corrispettivo una tantum*		*12.000,00 €*
Licenze per middleware di integrazione	*Corrispettivo una tantum*	192,40 €	*25.000,00 €*
Conduzione Applicativa - Servizi di gestione Applicativi e Base Dati (GAB) - *rif. documento 8.2.4 e 8.2.5*	GG/team ottimale	192,40 €	73.112,00 €
Servizi infrastrutturali – Conduzione Tecnica - *rif. documento 8.2.5*	GG/team ottimale	207,63 €	8.097,57 €
Manutenzione Adeguativa e Manutenzione Correttiva (MAD-MAC) - *rif. documento 8.2.5*	FTE/mese	3.884,30 €	23.305,80 €
Servizi di gestione operativa	canone		23.005,28 €
Totale			**435.834,21€**

Di seguito sono riportati dati, a valenza puramente indicativa, utilizzabili per il dimensionamento dei sistemi.

Ente Sanitario	N° Abitanti	N° Strutture Ospedaliere	N° SDO	N° Strutture Assistenziali Territoriali	N° Posti Letto	N° Assistiti	N° Personale
Azienda USL Umbria 1	491.039	7	21.469	173	574	492.410	3966
Azienda USL Umbria 2	368.533	10	25.018	220	935	368.533	3820
Azienda Ospedaliera di Perugia	N/A	1	33.260	N/A	754	N/A	3018
Azienda Ospedaliera di Terni	N/A	1	23.990	N/A	543	N/A	1740
Regione	859.572	19	103.737	393	2806	860.843	12.544

12 GESTIONE DELLA *PRIVACY* E DELLA SICUREZZA DELLE INFORMAZIONI

12.1 Protezione dei dati personali

Il trattamento dei dati personali derivante dalla prestazione dei servizi di cui al presente affidamento dovrà svolgersi nel rispetto delle norme in materia di protezione dei dati personali (di seguito, complessivamente, «Normativa Privacy»), ossia del Reg. UE 2016/679, recante il «Regolamento Europeo in materia di protezione dei dati personali» o «GDPR», del D.Lgs. 196/2003, recante il «Codice in materia di protezione dei dati personali» o «Codice Privacy», dei Provvedimenti emanati dalle Autorità competenti italiane ed europee, delle norme in materia di digitalizzazione rilevanti ai fini della data protection.

A titolo meramente esemplificativo, si richiamano:

- ***Norme fondamentali comunitarie e nazionali in materia di data protection:***

- Regolamento UE 2016/679, recante «*Regolamento Europeo in materia di protezione dei dati personali*»;
- Decreto Legislativo n. 196/2003, recante il «*Codice in materia di Protezione dei dati personali*», come novellato dal D.Lgs. 101/2018;
- ***Provvedimenti e prassi Ue in materia di data protection (a titolo esemplificativo):***
- «*Guidelines 9/2022 on personal data breach notification under GDPR*» dell'*European Data* Protection Board (in consultazione);
- «*Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*» dell'European Data Protection Board (in consultazione);
- «*Guidelines 01/2022 on data subject rights - Right of access*», adottate dall'European Data Protection Board il 18 gennaio 2022;
- «*Linee-guida 01/2021 su esempi riguardanti la notifica di una violazione dei dati personali*», adottate dall'European Data Protection Board il 14 dicembre 2021;
- Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato Economico e Sociale europeo e al Comitato delle Regioni «*relativa alla trasformazione digitale della sanità e dell'assistenza nel mercato unico digitale, alla responsabilizzazione dei cittadini e alla creazione di una società più sana*» (COM/2018/233/final del 25 aprile 2018);
- Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato Economico e Sociale europeo e al Comitato delle Regioni, recante «*Una strategia europea per i dati*» (COM/2020/66/final del 19 febbraio 2020);
- Raccomandazione della Commissione Europea dell'8 aprile 2020, recante «*on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data*»;
- *«Linee Guida 4/2019 in materia di Protezione dei dati fin dalla progettazione e per impostazione predefinita» adottate dall'European Data Protection Board il 20 ottobre 2020;*
- *«Linee-guida 03/2020 sul trattamento dei dati relativi alla salute a fini di ricerca scientifica nel contesto dell'emergenza legata al Covid-19», adottate dall'European Data Protection Board il 21 aprile 2020;*
- *«Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento possa presentare un rischio elevato ai fini del regolamento (UE) 2016/679», adottate dal WP29 il 4 aprile 2017 e modificate il 4 ottobre 2017;*
- *«Linee guida sul consenso ai sensi del regolamento (UE) 2016/679», adottate dal WP29 il 28 novembre 2017 e modificate il 10 aprile 2018;*
- *«Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679», adottate dal WP29 il 3 ottobre 2017 e modificate il 6 febbraio 2018;*
- *Provvedimenti e prassi nazionali in materia di data protection (a titolo esemplificativo):*
- *Provvedimento del 30 luglio 2019, adottato all'Autorità Garante per il trattamento dei dati personali, «sulla notifica delle violazioni dei dati personali (data breach)»;*

Fonti regolatorie in materia di digitalizzazione (a titolo esemplificativo):

- Decreto Legislativo 7 marzo 2005, n. 82, recante il «*Codice dell'amministrazione digitale*»
- «*Piano Triennale per l'informatica nella Pubblica Amministrazione 2020-2022*», approvato con D.P.C.M. 17 luglio 2020;
- «*Piano Nazionale di Ripresa e Resilienza*», approvato con Decisione di esecuzione del Consiglio dell'Unione europea del 13 luglio 2021;
- Determinazione AGID n. 628/2021 del 15 dicembre 2021, recante «*Regolamento recante i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la PA e le caratteristiche di qualità, sicurezza, performance e scalabilità, portabilità dei servizi cloud per la pubblica amministrazione, le modalità di migrazione, nonché le modalità di qualificazione dei servizi cloud per la pubblica amministrazione*»;
- Circolare AGID 18 aprile 2017, n. 2/2017, recante: «*Misure minime di sicurezza ICT per le pubbliche amministrazioni*»;
- Legge 9 gennaio 2004, n. 4, recante «*Disposizioni per favorire e semplificare l'accesso degli utenti e, in particolare, delle persone con disabilità agli strumenti informatici*»;
- Circolare del 9 aprile 2018, n. 2, adottata dall'Agenzia Digitale per l'Italia, e avente ad oggetto «*Criteri per la qualificazione dei Cloud Service Provider per la PA*»;
- Circolare AGID del 1° ottobre 2018, n. 3, avente ad oggetto «*Responsabile per la transizione digitale - art. 17 decreto legislativo 7 marzo 2005, n. 82 "Codice dell'amministrazione digitale"*»;
- «*Linee guida AGID sull'accessibilità degli strumenti informatici*», adottate il 23 luglio 2020;
- «*Linee Guida AGID sulla formazione, gestione e conservazione dei documenti informatici*», adottate a settembre 2020 e modificate a maggio 2021;
- Determinazione AGID n. 455/2021 del 25 giugno 2021, recante «*Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici*».

Si precisa che il Fornitore, nel corso dell'intera durata del contratto, dovrà garantire pieno rispetto anche delle norme, dei provvedimenti e delle prassi in materia di data protection che dovessero intervenire nel tempo.

Fermo quanto sopra, nei sottoparagrafi successivi si descriveranno alcuni degli obblighi generali (connessi alla Normativa Privacy) e specifici (individuati sulla base delle peculiarità degli appalti oggetto di affidamento con la presente procedura) che il Fornitore dovrà rispettare ai fini della protezione dei dati personali. Tutto quanto definito e richiesto dal presente Capitolato Tecnico dovrà essere garantito dal Fornitore e dai suoi eventuali subappaltatori/subcontraenti.

12.1.1 Obblighi generali del Fornitore in materia di protezione dei dati personali

Il Fornitore verrà nominato responsabile del trattamento dei dati personali (di seguito, anche solo «**Responsabile**») dal titolare del trattamento (di seguito, anche «**Titolare**»), e dovrà, pertanto, operare in conformità alle prescrizioni di cui all'art. 28 del GDPR, alle previsioni afferenti alla data protection che saranno contenute nel Contratto Esecutivo e alle istruzioni che saranno impartite dal Titolare medesimo nel corso dell'esecuzione dell'appalto.

In ragione di quanto sopra e a titolo esemplificativo, il Fornitore dovrà:

- **Sul piano organizzativo**: strutturare e mettere in atto un'organizzazione specifica per la protezione dei dati personali attraverso la definizione di un modello privacy, con individuazione di ruoli, funzioni e responsabilità, procedendo alla predisposizione delle necessarie policy e al conferimento delle nomine.

In tal senso, procederà ad individuare: (i) i soggetti "delegati" e i soggetti "autorizzati" al trattamento", ai sensi dell'art. 2-*quaterdecies* del Codice Privacy; (ii) gli "Amministratori di sistema" per le attività legate al presente appalto (v. Provvedimento del 27 novembre 2008). Il Fornitore avrà facoltà di avvalersi di sub-fornitori, nelle modalità previste dall'art. 28 Reg. UE 2016/679 e dal Contratto Esecutivo;

- **Sul piano delle misure di sicurezza**: il Fornitore dovrà adottare un approccio basato sul principio di Privacy by Design e by Default di cui agli artt. 25 e 32 del GDPR e alle «*Guidelines* 4/2019 *on Article 25 Data Protection by Design and by Default*», adottate dall'*European Data Protection Board* (EDPB) il 20 ottobre 2020. Di conseguenza, il Fornitore dovrà:
    - da un lato, predisporre fin dalla progettazione misure tecniche e organizzative adeguate (*data protection by design*), volte (i) ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e (ii) ad integrare nel trattamento le garanzie necessarie a soddisfare i requisiti del GDPR e a tutelare i diritti e le libertà fondamentali degli interessati;
    - dall'altro, dare effettiva attuazione alle suddette misure nell'ambito del trattamento, affinché siano trattati, per impostazione predefinita, solo i dati personali necessari alla specifica finalità perseguita (*data protection by default*).

In tal senso, il Fornitore, nel valutare l'adeguato livello di sicurezza, dovrà tenere conto dei rischi presentati dal trattamento, in particolare di quelli che derivano dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.
In caso di violazione dei dati personali, nel rispetto del GDPR e del Contratto Esecutivo, il Fornitore dovrà
a) darne comunicazione al Titolare, immediatamente e, in ogni caso, non oltre le 24 ore, da quando il Fornitore medesimo, o un suo Sub-Responsabile, ha avuto conoscenza della violazione o ha avuto elementi per sospettare che sia avvenuta una violazione;

b) collaborare con il Titolare, anche al fine di consentire il completamento del processo di notifica all'Autorità Garante, nelle (i) attività di indagine, al fine rilevare tutte le evidenze necessarie a valutare le cause, la natura e gli effetti della violazione dei dati personali, nonché (ii) nell'adozione delle azioni necessarie a mitigare qualsivoglia danno o conseguenza lesiva per i diritti e delle libertà degli Interessati e (iii) nella predisposizione e implementazione, previa approvazione del Titolare, di un piano di misure per la riduzione tempestiva delle probabilità che una violazione dei dati personali simile a quella occorsa possa ripetersi in futuro.

12.1.2 Previsioni specifiche in materia di protezione dei dati personali

A specificazione e in aggiunta rispetto agli obblighi generali di cui al paragrafo precedente, il Fornitore dovrà:

(a) garantire il pieno coordinamento con gli altri soggetti coinvolti nel trattamento dei dati personali – quali, ad esempio, Regione, Ministero della Salute, Istituto Superiore di Sanità, Operatori e Strutture sanitarie – proponendo misure tecnico-giuridiche finalizzate alla integrazione e alla sinergia con gli stessi (ad es., procedure, protocolli operativi). Tali strumenti dovranno assicurare la conformità dei trattamenti alla Normativa Privacy nel corso dell'intero ciclo di vita dei dati personali ed efficaci policy in materia di privacy, ad esempio con riferimento alla gestione degli eventi di data breach, in modo di consentire al Titolare di porre in essere le attività previste dalla Normativa Privacy medesima;

(b) garantire il rispetto della data protection nell'ambito dell'intero ciclo di vita dei dati personali, anche mediante misure tecnico-organizzative differenziate a seconda del soggetto di volta in volta coinvolto (ad es., MMG/PLS, Medico Specialista, ecc.). A tal fine, il Fornitore dovrà tra l'altro garantire adeguata formazione nei confronti di ciascuna tipologia di soggetti coinvolti nei processi di digitalizzazione e predisporre apposite linee guide, manuali, moduli, flussi relativi ai processi e al ciclo di vita del dato;

(c) individuare una figura che ricopra il ruolo di Privacy & Security Manager, che gestirà nel corso dell'esecuzione contrattuale tutte le tematiche di Sicurezza e di Privacy afferenti alla commessa e che costituirà il referente unico per l'Azienda in merito alle suddette materie;

(d) garantire il rispetto della normativa in materia di digitalizzazione (ad es., CAD e Linee Guida AGID), quali, ad esempio, le «*Linee Guida AGID sulla formazione, gestione e conservazione dei documenti informatici*» di settembre 2020/maggio 2021; la Determinazione AGID n. 628/2021 del 15 dicembre 2021 in materia di «*Cloud della PA*» e il Provvedimento del Garante n. 393 del 2 luglio 2015, in materia di «*Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche*»;

(e) supportare sul piano tecnico il Titolare nelle interlocuzioni con l'Autorità garante per la protezione dei dati personali, l'Agenzia per l'Italia Digitale, il Ministero della Salute, l'Agenzia per la Cybersicurezza Nazionale, ed ogni altra Autorità coinvolta nell'ambito dell'attuazione dell'appalto in questione;

(f) effettuare specifiche analisi del rischio privacy (sulla base del principio di *privacy by design*), al fine di segnalare, in qualsiasi momento, al Titolare rischi originari e/o sopravvenuti connessi al trattamento e di individuare misure tecniche ed organizzative da adottare, anche ai fini di una effettiva e costante tutela dei diritti e delle libertà delle persone fisiche; (g) supportare il Titolare nello svolgimento *ex ante* delle valutazioni d'impatto sulla protezione dei dati personali (o «**DPIA**») in merito ai trattamenti che saranno posti in essere ai fini dell'esecuzione delle prestazioni oggetto

di affidamento, conformemente all'articolo 35 del Regolamento (UE) n. 2016/679 e alle migliori prassi UE e nazionali.

Il Fornitore, al fine di individuare eventuali criticità per ciò che concerne la Normativa Privacy e di apportare i necessari correttivi, dovranno effettuare e trasmettere al Titolare specifiche analisi del rischio anche sui prodotti software, in fase di progettazione e prima del loro sviluppo;

(h) adottare, nell'ambito della progettazione dei sistemi, (i) misure idonee a garantire la "qualità ed esattezza del dato" (ossia la completezza, accuratezza, tempestività, coerenza, univocità, integrità, conformità dello stesso), (ii) nonché processi idonei a monitorare costantemente i flussi relativi ai processi e al ciclo di vita dei dati, segnalando immediatamente con appositi alert qualsiasi anomalia effettiva o potenziale;

(i) adottare misure per l'acquisizione e la conservazione dei consensi (ove necessari in ragione degli specifici trattamenti, alla luce dei «*Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario*» resi dal Garante in data 7 marzo 2019) nel rispetto del GDPR (i.e., art. 7) e delle prassi UE e nazionali

12.2 Gestione della sicurezza delle informazioni

Di seguito vengono riportate le misure di sicurezza atte a preservare l'integrità, la disponibilità e la riservatezza dei servizi e delle informazioni che dovranno essere attuate dal Fornitore nell'ambito delle attività ad esso assegnate. Il Fornitore dovrà garantire e monitorare l'applicazione delle prescrizioni di seguito descritte anche da parte degli eventuali suoi sub-fornitori, anche attraverso attività di audit.

Requisiti generali

Il Fornitore dovrà:

- Garantire la riservatezza, l'integrità e la disponibilità delle informazioni gestite nell'ambito di tutte le attività ad esso affidate;
- Nell'ambito del trattamento dei dati e delle informazioni, ed in particolare nella comunicazione e trasmissione di informazioni, all'interno e all'esterno dell'organizzazione rispettare il principio di:
  - Least privilege;
  - Need-to-know;
  - Segregation of duties.
- Collaborare attivamente con il Titolare nell'applicazione delle misure di sicurezza previste;
- Garantire, e/o collaborare a, la redazione di tutta la documentazione di Sicurezza e Privacy, in conformità agli standard definiti;
- Utilizzare le procedure operative del Titolare al fine di assicurare la sicura e corretta operatività delle strutture di elaborazione delle informazioni del Titolare e, laddove il Fornitore operasse presso la propria sede e con proprie risorse deve documentare, aggiornare e curare la messa in pratica di

adeguate procedure operative e documentare e monitorare tutti i cambiamenti apportati alle strutture di elaborazione delle informazioni e ai sistemi;

• Prevedere la designazione di una figura che ricopra il ruolo di Security Manager, indicativamente corrispondente al profilo professionale Cloud Security Specialist definito dall'AQ, in termini di "focal point" per le tematiche di Sicurezza e Privacy, per la gestione degli eventuali eventi anomali, incidenti e sulle tematiche tecnologiche ed organizzative ovvero ad un eventuale piano di continuità operativa del Titolare, ivi comprese le attività di Disaster Recovery.

Requisiti di riservatezza

Il Fornitore dovrà:

- Utilizzare i dati personali e le informazioni in modo lecito e secondo correttezza, per scopi legittimi e determinati, nel rispetto del principio di pertinenza e non eccedenza rispetto alle attività svolte;
- Utilizzare i dati personali e le informazioni solo ed esclusivamente per le attività connesse all'esecuzione di quanto richiesto contrattualmente;
- Non trattare i dati personali, ovvero le informazioni, diversi da quelli per i quali è stato espressamente autorizzato;
- Garantire il rispetto della riservatezza, dell'integrità e della disponibilità dei dati personali e delle informazioni adottando tutte le misure, fisiche nonché tecnologiche, di sicurezza idonee;
- Mantenere strettamente riservati i dati personali e le informazioni trattati nello svolgimento di quanto richiesto contrattualmente, non diffonderli e non comunicarli a terzi salvo preventiva autorizzazione scritta del Titolare. L'obbligo di riservatezza in merito ai dati vincolerà il Fornitore, i suoi dipendenti, collaboratori, consulenti e sub-fornitori, per tutta la durata del contratto e per i cinque anni successivi alla data della sua cessazione, per qualunque causa essa sia avvenuta;
- Non copiare, duplicare, riprodurre o registrare, in qualsiasi forma e con qualsiasi mezzo, i dati e le informazioni, salvo nella misura strettamente necessaria per l'esecuzione dell'attività richiesta e sempre previa autorizzazione scritta da parte del Titolare; al termine delle attività richieste o comunque del contratto, restituire al referente del Titolare i dati e le informazioni oppure, se richiesto e applicabile, procedere alla loro distruzione, con modalità sicure e documentate, fornendone evidenza;
- Comunicare immediatamente al referente del Titolare qualunque evento che abbia violato o posto in pericolo la riservatezza, l'integrità e la disponibilità dei dati personali e delle informazioni;
- Cancellare in maniera sicura, secondo le tecnologie più adeguate, i dati e le informazioni presenti sui dispositivi (PC, Tablet, ecc.) in caso di dismissione e comunque al termine del contratto. Tutte le attività di dismissione sicura dovranno essere registrate e conservate fornendo al Titolare tutte le evidenze di quanto svolto durante tutto l'arco del contratto;
- Nel caso in cui l'attività di manutenzione debba essere svolta all'esterno del Titolare, garantire che i dati personali e le informazioni contenute nei prodotti non siano accessibili;
- Definire ed attuare delle procedure per il loro trattamento e memorizzazione dei dati e delle informazioni. Nello specifico il Fornitore dovrà adottare idonee procedure per la gestione,

mantenimento e dismissione dei supporti di memorizzazione contenenti dati, ad esempio implementando metodi di sovrascrittura a più livelli o cancellazione sicura dei supporti. Tutte le attività di dismissione sicura dovranno essere registrate e conservate fornendo al Titolare tutte le evidenze di quanto svolto durante tutto l'arco del contratto.

- È sempre vietata l'estrazione e il trasferimento di dati e/o di ogni altra informazione dalle basi dati e dai sistemi del Titolare, salvo espressa e preventiva autorizzazione scritta.

Gestione del personale del Fornitore

Il Fornitore dovrà garantire che il proprio personale (dipendenti e collaboratori), abbia piena consapevolezza delle problematiche relative alla sicurezza delle informazioni. In particolare:

- Il Fornitore, durante il processo di acquisizione del proprio personale, dovrà valutare i livelli di conoscenza degli obiettivi e delle problematiche di sicurezza in funzione delle attività che dovranno essere svolte. Inoltre, il personale del Fornitore dovrà ricevere da questi un'adeguata e continuativa formazione inerente alle tematiche di Sicurezza e Privacy;
- Il Fornitore, alla conclusione del rapporto di lavoro del dipendente e/o collaboratore, dovrà: o Nel caso in cui le credenziali siano definite sulle reti, sistemi e applicazioni del Titolare, comunicare tempestivamente al referente del Titolare i nominativi degli utenti che dovranno essere rimossi;
    - Nel caso in cui le credenziali siano definite sulle reti, sistemi e applicazioni gestite dal Fornitore, rimuovere tutte le credenziali di autenticazione (ID e password) utilizzate dal dipendente e/o collaboratore dimissionario.

Accesso agli ambienti ed ai sistemi

Accesso agli ambienti del Titolare

Il Fornitore potrà accedere alle reti, ai sistemi e agli ambienti che il Titolare metterà a disposizione, relativamente al proprio ambito di competenza, attraverso le modalità di connessione definite.
L'infrastruttura utilizzata dovrà rispettare i requisiti minimi definiti e descritti nel seguito.
In nessun caso, in ambienti diversi dalla produzione, dovranno essere presenti dati reali di produzione dei servizi gestiti, a meno di preventiva autorizzazione scritta fornita dal Titolare. Si sottolinea che, ancorché salvaguardate le problematiche di protezione dei dati personali, il Fornitore rimane responsabile del rischio di furto, perdita accidentale e/o distruzione di patrimonio informativo, inteso come le basi dati, il codice sorgente e/o le soluzioni prodotte, le infrastrutture e le personalizzazioni sviluppate nonché le informazioni e i dati trattati, per quanto di sua competenza.

Accessi logici

Il Fornitore dovrà garantire sia sugli ambienti del Titolare da esso gestiti, sia sui propri ambienti, che l'accesso alle informazioni, servizi e sistemi avvenga in modo sicuro per prevenire l'accesso da parte di utenti che non hanno i necessari diritti e pertanto impedire trattamenti non autorizzati.
Il ciclo di vita delle utenze, sui sistemi gestiti dal Fornitore, prevede che:

- Ogni operazione del ciclo di vita (creazione, modifica, sospensione, ecc.) che riguarda le utenze relative ad ambienti, sistemi o applicazioni del Titolare, dovrà essere preventivamente formalizzata dal Fornitore ai referenti specifici del Titolare e da questi ultimi autorizzata;
- Il Fornitore dovrà effettuare la tracciatura di tutte le richieste effettuate inerenti alla gestione del ciclo di vita delle utenze per renderla disponibile su richiesta.

Accesso a reti, sistemi e ambienti del Titolare

Nel caso di accesso a reti, sistemi e ambienti del Titolare, il Fornitore dovrà:

- Richiedere in forma scritta la creazione di una nuova utenza che dovrà contenere l'identificativo della persona a cui verrà assegnata, l'ambito di utilizzo, il ruolo, l'ambiente e la durata. Le utenze richieste dovranno essere univoche, personali e utilizzate in modo che l'accesso alle informazioni da parte di ogni singolo utente sia limitato alle sole (principio del "minimo privilegio") informazioni di cui necessita (principio del "need-to-know") per lo svolgimento dei propri compiti;
- Inviare una tempestiva comunicazione in caso di variazione delle mansioni o delle attività in modo che il profilo venga adeguato alle effettive nuove esigenze; effettuare una revisione periodica delle utenze al fine di individuare le utenze inattive e quelle che necessitano di una modifica;
- Richiedere immediatamente la disabilitazione di un'utenza assegnata ad un suo dipendente o collaboratore nei seguenti casi:
- Interruzione del rapporto di lavoro con il Fornitore;
- Cambio di mansione che non necessita dell'accesso ai sistemi informatici /applicazioni del Titolare;
- Utenze inattive emerse nella revisione periodica.
- Tutto il personale autorizzato del Fornitore dovrà:
- Eseguire l'accesso ai sistemi e agli ambienti tramite le proprie credenziali di accesso personali (ad esempio user ID, password) fornite dal Titolare;
- Custodire ed utilizzare le proprie credenziali di accesso con la massima cautela al fine di evitare l'intercettazione, volontaria o fortuita, delle stesse da parte di terzi evitando in ogni caso di comunicarle ad altri e non consentendo a nessun'altra persona di utilizzarle.

Accesso ad ambienti del Fornitore

Nel caso in cui il Fornitore tratti dati e/o informazioni del Titolare attraverso propri ambienti e sistemi dovrà:

- Rispettare principi espressi nei Paragrafi precedenti relativamente alla gestione del ciclo di vita delle utenze e all'accesso alle informazioni;
- Definire un processo di gestione delle credenziali di autorizzazione e dei relativi profili di accesso;
- Definire utenze univoche, personali e profilate inottemperanza alle normative di riferimento;
- Definire le autorizzazioni di accesso alle informazioni in modo che siano differenziate in base al ruolo e dagli incarichi ricoperti dai singoli individui;
- Definire le procedure per consentire l'accesso ai dati nei casi in cui, a causa della prolungata assenza o dell'impedimento della persona autorizzata, si renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del Titolare;

- Effettuare periodicamente valutazioni tecniche sulla robustezza delle parole chiave usate dagli utenti;
- Provvedere alla sospensione delle utenze nei seguenti casi:
  - Assenza prolungata del dipendente (assenza per malattia o infortunio superiore a 90 giorni);
  - Scadenza della parola chiave e inserimento consecutivo di 5 parole chiave errate;
  - Decorrenza del tempo massimo di inattività;
  - Scadenza di un'utenza temporanea, utilizzata da personale non dipendente.

- Formalizzare e tracciare la richiesta di riattivazione di un'utenza sospesa. Inoltre, qualora il ripristino avvenga a seguito di sospensione per scadenza temporale della parola chiave, consentire all'utente di accedere al sistema solo per modificare la password;
- Gestire la storicizzazione degli account e delle loro attività al fine di tenerne traccia, fornendo, su richiesta del Titolare le informazioni in merito.
- Tutte le persone autorizzate del Fornitore dovranno:
- Eseguire l'accesso ai sistemi e ambienti del Fornitore tramite le proprie credenziali di accesso personali (ad esempio user ID, password);
- Custodire ed utilizzare le proprie credenziali di accesso con la massima cautela al fine di evitare l'intercettazione, volontaria o fortuita, delle stesse da parte di terzi evitando in ogni caso di comunicarle ad altri e non consentendo a nessun'altra persona di utilizzarle.

Modalità e specifiche di connessione

La connessione remota (dove per remota è da intendersi eseguita da sedi non del Titolare) ai sistemi del Titolare è permessa solo attraverso:

- Connessioni dedicate;
- Connettività Virtual Private Network (VPN) di tipo site-to-site.

La connettività VPN-Client, che deve essere nominale, è autorizzata solo in casi eccezionali e corredata da opportuna motivazione scritta.
La connettività Internet e l'apparato remoto lato Fornitore saranno a suo carico così come pure la configurazione della connessione VPN nel caso di connettività site-to-site.
Il Titolare deve fornire le specifiche di configurazione, a cui la connettività VPN deve rispondere, che dovranno essere applicate dal Fornitore. La VPN deve essere unica per ciascun Fornitore (nel caso di Raggruppamento Temporaneo d'Impresa (RTI) e resa disponibile una VPN per ogni società appartenente all'RTI). Non sono possibili in nessun caso VPN multiple per lo stesso Fornitore.

Infrastruttura

Il Fornitore, in funzione delle attività assegnate, deve implementare le opportune regole di sicurezza in funzione della criticità del servizio e/o dell'informazione trattata.
Nel dettaglio il Fornitore deve, ove ricorra il caso:
• Garantire la separazione degli ambienti (es: sviluppo, integrazione, test, produzione, management);

• Prevedere meccanismi di autenticazione forte per l'accesso agli ambienti, qualora le esigenze di sicurezza lo richiedano;

• Implementare opportuni meccanismi di tracciatura e auditing;

Controllare e monitorare, tramite appositi strumenti (quali ad esempio firewall, IDS, Correlatori di Eventi, ecc.), gli eventuali "punti di contatto" tra le reti interne del Fornitore e la rete del Titolare;

• Garantire lo svolgimento di attività di backup e restore secondo procedure formalizzate che definiscano le metodologie di salvataggio e ripristino, i tempi di conservazione delle copie, il numero di versioni da salvare e la tipologia dei dati. In particolare, per i sistemi critici, dovranno essere periodicamente effettuati salvataggi dei file di sistema e di tutti quelli necessari per il ripristino degli stessi e di eventuali applicativi rilevanti ai fini della continuità delle operazioni;

• Prevedere con cadenza periodica, al fine di garantire efficienza e livelli di sicurezza adeguati ai sistemi utilizzati:

o Attività di hardening;

o Attività di patching;

o Vulnerability assessment/penetration test e relativo piano di trattamento.

• Verificare periodicamente i sistemi e le procedure di backup e restore in tutte le loro componenti e funzionalità, sia in condizioni di normale operatività che in condizioni di emergenza. In particolare, dovranno essere condotti dei test di ripristino dei salvataggi effettuati;
• Conservare in luoghi sicuri opportunamente protetti i supporti utilizzati per eseguire backup. Il tempo di mantenimento dei dati deve essere compatibile con le esigenze del Titolare e con la Normativa Privacy;
• Verificare con regolarità la conformità dei sistemi informativi, servizi e applicazioni agli standard di sicurezza e ai requisiti richiesti dal Titolare e dalle normative di riferimento.

Relativamente agli ambienti di sviluppo, qualora richiesto dal Titolare, il Fornitore deve:
• Predisporre in casa propria tutti gli ambienti di sviluppo necessari;

• Verificare che, in nessun caso, siano presenti dati reali o riconducibili a persone fisiche realmente esistenti;

• Prevedere opportuni allineamenti dei codici sorgente sviluppati presso le proprie sedi, con gli strumenti di versioning del codice sorgente sviluppato.

Relativamente agli strumenti di lavoro, il Fornitore deve:

Dotare le postazioni di lavoro utilizzate per accedere alla rete e ai sistemi del Titolare (ove applicabile) di opportuni meccanismi di sicurezza (antivirus, patch di sicurezza, ecc.) e segregarle dal resto della rete del Fornitore;

• Utilizzare sistemi antivirus, controllo malware e meccanismi di sicurezza per i media rimovibili, per tutti i sistemi, postazioni e reti;

• Garantire che tutti gli strumenti di lavoro introdotti, come ad esempio laptop e dispositivi di memorizzazione usati dalle persone autorizzate del Fornitore, siano stati preventivamente autorizzati e dotati di tutte le misure di sicurezza ritenute necessarie e adeguate in conformità con gli standard vigenti presso il Titolare;

• Garantire che su tutti gli strumenti di lavoro, anche su quelli eventualmente forniti dal Titolare, non sia installato software e/o modificata la configurazione dei sistemi senza preventiva autorizzazione scritta;

• Consentire l'esecuzione di controlli da parte del Titolare volti a garantire la riservatezza, l'integrità e la disponibilità dei dati e delle informazioni, anche tramite l'utilizzo di strumenti informatici che saranno preventivamente comunicati al Fornitore;

• Consentire l'installazione sulle proprie postazioni di lavoro di componenti software, preventivamente comunicati al Fornitore, necessari per assicurare una connessione sicura alla rete del Titolare;

• Non lasciare incustodita la postazione di lavoro e nel caso, prima di allontanarsi, assicurarsi di chiudere le eventuali sessioni aperte e di attivare lo screensaver con password.
Al Fornitore non è consentito l'uso di dispositivi mobili (smartphone, tablet, ecc.) propri o aziendali per l'accesso ai dati e informazioni del Titolare se non preventivamente richiesto al Titolare e dal Titolare espressamente autorizzato.

Analisi e gestione dei rischi

Ove richiesto dal Titolare, il Fornitore è tenuto a svolgere attività di analisi dei rischi rispetto alla sicurezza delle informazioni sull'intero oggetto del contratto.
I risultati dell'analisi dei rischi dovranno essere presentati al Titolare dal Fornitore nei tempi e nei modi che saranno concordati opportunamente tra le parti e dovranno almeno prevedere:

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

Il documento dovrà essere aggiornato ove dovessero intervenire eventi/circostanze impattanti sul contenuto e di tali variazioni dovrà essere data evidenza al Titolare.
Il Fornitore, condividendolo con il Titolare, definirà, ove necessario, le modalità di gestione del rischio (ovvero mitigazione, esternalizzazione ed accettazione) e sarà responsabile della redazione di un Piano di Trattamento dei Rischi da attuare nei tempi concordati con il Titolare.

Sicurezza fisica

Il Fornitore, al fine di garantire a tutte le informazioni e a tutti i dati gestiti per conto del Titolare adeguati livelli di tutela, dovrà definire, implementare e mantenere opportune soluzioni di sicurezza relativamente a: sicurezza perimetrale, controllo degli accessi fisici, sicurezza di uffici, locali tecnici ed attrezzature e quanto necessario. Ad esempio, l'alimentazione elettrica e la sicurezza dei cablaggi, i supporti di memorizzazione in ingresso e in uscita, lo smaltimento e il riutilizzo delle apparecchiature stesse.

Per le attività svolte presso le sedi o CED del Titolare, il Fornitore si impegna a rispettare le istruzioni e misure di sicurezza comunicate dal Titolare stesso.

Gestione degli eventi anomali, degli incidenti e della Business Continuity

Il Fornitore dovrà garantire che le anomalie e gli incidenti aventi ripercussioni sul sistema informativo e sui livelli di sicurezza, siano tempestivamente riconosciuti e correttamente gestiti attraverso efficienti sistemi di prevenzione, comunicazione e reazione, per minimizzare l'impatto sul business.

È fatto obbligo al Fornitore di una altrettanto tempestiva notifica nei confronti del Titolare degli eventi anomali e/o incidenti di sicurezza che coinvolgono sistemi del Fornitore che contengono o trattano dati o codice del Titolare.
Nel dettaglio il Fornitore dovrà:

- Implementare le procedure di gestione degli incidenti di sicurezza e di comunicazione degli stessi al Titolare;
- Rilevare gli incidenti che possano avere un impatto sui livelli di sicurezza. Dovrà altresì garantire la completa gestione degli eventuali effetti, reali o potenziali, derivanti dall'incidente, ove possibile in tempi brevi, garantendo il rispetto delle procedure, ove presenti o definite, sempre in accordo con il Titolare;
- Prevedere un sistema di registrazione e classificazione degli incidenti e degli eventi anomali per effettuare analisi volte al miglioramento dei livelli di sicurezza coerente con le reali problematiche riscontrate;
- Raccogliere le evidenze a seguito di un incidente di sicurezza, conservarle e presentarle qualora sussista la necessità di azioni legali di natura civile o penale;
- Attivare e mantenere idonee procedure di Business Continuity nella misura ed in relazione al servizio prestato al Titolare, in coerenza con i livelli di servizio previsti dal contratto;
- Concorrere all'attivazione e al coordinamento dei gruppi operativi del proprio personale dedicato alla gestione delle emergenze e della crisi comunicandolo al Titolare e tenendo aggiornati i nominativi e i recapiti che garantiscano la pronta rintracciabilità delle figure competenti individuate; dovrà partecipare ai test tecnici e organizzativi di Business Continuity e di Disaster Recovery, per quanto di competenza.

Rispetto delle procedure di sicurezza

Il Fornitore si impegna a rispettare le procedure di sicurezza del Titolare.
Il rispetto delle procedure di sicurezza e di qualsiasi loro modifica introdotta dal Titolare, anche durante il corso della fornitura, è sempre parte integrante della Fornitura stessa. Il Fornitore non potrà avanzare richieste di estensione contrattuale o pagamenti specifici connessi a questo specifico ambito.

Report da parte del Fornitore

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

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

Una volta approvato il documento da parte del Titolare, il Fornitore dovrà, mediante lo stesso o altro documento di rendiconto previsto dal Titolare, autocertificare, annualmente o su richiesta del Titolare, il rispetto delle regole e delle policy relative alla sicurezza delle informazioni. Questa documentazione è considerata parte del sistema complessivo di monitoraggio della Fornitura.

Attività di verifica e controllo

Il Titolare avrà facoltà di effettuare attività di verifica e controllo sull'applicazione, da parte del Fornitore ed eventualmente dei sub-fornitori, di quanto sopra esposto e di qualsiasi altra misura di sicurezza che dovrà

essere successivamente definita a fronte di eventuali evoluzioni e/o modifiche normative o standard di settore. La verifica può essere effettuata sia tramite visita presso il Fornitore o, congiuntamente, presso i suoi sub-fornitori, sia tramite richiesta di idonea documentazione attestante la conformità ai requisiti di sicurezza richiesti contrattualmente nonché dalla normativa di riferimento e successive modifiche.
A fronte di difformità rilevate, il Fornitore si impegna ad eseguire gli interventi per il superamento delle stesse previa validazione da parte del Titolare delle soluzioni identificate.

Deroghe

In casi straordinari e con le dovute autorizzazioni opportunamente documentate sarà possibile operare in deroga alle regole di sicurezza qui stabilite.
Le richieste da parte del Fornitore dovranno essere formalizzate e tracciate, oltre che adeguatamente documentate. In particolare, dovranno essere esplicitate le motivazioni che giustificano la deroga, gli ambiti operativi e temporali di intervento, l'identificazione del personale esterno e le attività da autorizzare.
La richiesta dovrà essere indirizzata agli specifici referenti operativi del Titolare che provvederanno, coinvolgendo le opportune strutture aziendali interne, ad ottenere autorizzazione scritta per le richieste ammissibili.

Reperibilità

Il Fornitore è tenuto a comunicare i numeri di reperibilità relativi alle figure di Security Manager, a garanzia di una corretta e tempestiva erogazione di tutti i servizi a suo carico, di cui viene riportato di seguito un elenco esemplificativo, ma non esaustivo:

- Comunicazione e gestione di incidenti di sicurezza;
- Comunicazione e gestione di eventi di data breach;
- Test tecnici e/o organizzativi di Disaster Recovery;
- Attivazione dei servizi in Disaster Recovery;
- Piano di rientro dal Disaster Recovery.
- La reperibilità per tale figura è da intendersi 24x7x365.