PROPOSTA DI PARTNERSHIP PUBBLICO PRIVATO
ai sensi degli artt. 180 e 183, c. 15, del Decreto legislativo 18 aprile 2016, n. 50
per l'AFFIDAMENTO DELLA CONCESSIONE per la progettazione, realizzazione e gestione dei Servizi Abilitanti della Piattaforma Nazionale di Telemedicina
PNRR - Missione 6 Componente 1 sub-investimento 1.2.3. "Telemedicina"

Progetto Tecnico dell'Architettura dei Servizi ("PTAS")

PPP Telemedicina - PTAS - Indice dei contenuti

1. Contesto

AGENAS, in qualità di Soggetto Attuatore per la progettazione, la realizzazione e la gestione dei Servizi Abilitanti della Piattaforma Nazionale di Telemedicina nell'ambito del PNRR - Missione 6 Componente 1 *sub*-investimento 1.2.3 "*Telemedicina*", ha avviato, mediante avviso pubblico (l'"**Avviso**"), un procedimento finalizzato ad acquisire dal mercato proposte ad iniziativa privata (le "**Proposte**"), *ex* art. 183, comma 15 e ss. del D.Lgs. 50/2016 e ss.mm.ii. (il "**Codice dei Contratti Pubblici**" o "**Codice**"), da parte di operatori economici (l'/gli "**OE**"), adeguatamente qualificati ed in possesso di requisiti idonei ai sensi di legge (i "**Proponenti**").

Come si evince dall'Avviso, **le Proposte dovevano avere ad oggetto la progettazione, la realizzazione e la gestione dei Servizi Abilitanti della Piattaforma Nazionale di Telemedicina (la "PNT" o la "Piattaforma"), *sub*-investimento 1.2.3, nell'ambito della Missione 6 Componente 1 del PNRR.**

Nella stesura del PTAS, l'intervento è stato, pertanto, congetturato attenendosi strettamente ai criteri che seguono:

- con un peso estremamente rilevante:
  - interoperabilità e semplicità di integrazione con i servizi di telemedicina;
  - adozione delle codifiche di normazione nazionali ed internazionali;
  - adozione delle linee guida e dei PDTA al fine di ottemperare quanto previsto dalle norme sulla appropriatezza prescrittiva;
  - *cybersecurity*, intesa come soluzioni tecnologiche, *upgrade* e servizi atti a minimizzare il rischio di *cybersecurity* e/o ad assicurare il tempestivo ripristino del pieno funzionamento della Piattaforma;
- con un peso molto rilevante:
  - coerenza con le altre progettualità nazionali ed internazionali, in particolare l'FSE 2.0 e la nuova normativa che introduce la EHDS (*European Health Data Space*), di cui sono già disponibili i documenti al fine di procedere negli *step* approvativi per giungere, come previsto, alla emissione del regolamento europeo atteso entro il 2023;
  - flessibilità, affidabilità, robustezza (anche in condizioni critiche) e scalabilità dell'architettura logica e fisica della Piattaforma, aggiornamento continuo dei componenti tecnologici;
- ed, infine, con un peso rilevante:

- scelte tecnologiche atte a ridurre il rischio di *lock-in*;
- efficacia del modello organizzativo;
- governo del rischio di disponibilità, con riferimento anche agli indicatori di applicazione delle decurtazioni ed efficienza ed ottimizzazione della struttura dei costi, quest'ultimo affrontato nel documento gestionale.

Il PTAS mantiene una stretta aderenza a *standard* nazionali ed internazionali, insieme alle pratiche che, per la loro diffusione, possono rappresentare degli *standard de facto*.

Nell'Avviso, nell'allegato tecnico allo stesso (l'"Allegato") e negli incontri informativi, è stato specificato che la PNT è un "*insieme di diversi servizi che cooperando ed interoperando in sinergia realizzano i servizi finali per pazienti ed operatori, garantendo ai diversi livelli di governo coinvolti il monitoraggio dei processi*". I servizi che devono essere garantiti sono l'architettura e l'infrastruttura logico-fisica necessaria sopra la quale i "*Servizi Abilitanti*" sono realizzati e tutti i servizi di supporto necessari al buon funzionamento degli stessi.

Il modello logico-funzionale previsto nell'Avviso considera che l'ecosistema digitale per il supporto dei processi di telemedicina debba essere costituito da servizi *ICT*. In tale contesto, tuttavia, risulta fondamentale la indipendenza, scalabilità e facilità di integrazione tra i diversi processi e con i servizi già sviluppati ed utilizzati dalle regioni per garantire che gli investimenti già attuati o programmati siano parte di una strategia nazionale.

La PNT è composta da "*Servizi Abilitanti*" e si integra con i "*Servizi Minimi di Telemedicina*" (*regionali e non inclusi in questa progettualità*). I Servizi Minimi di Telemedicina sono attuati a livello regionale, raccordandosi, in modo armonico, con gli ecosistemi digitali specifici di ogni Regione.

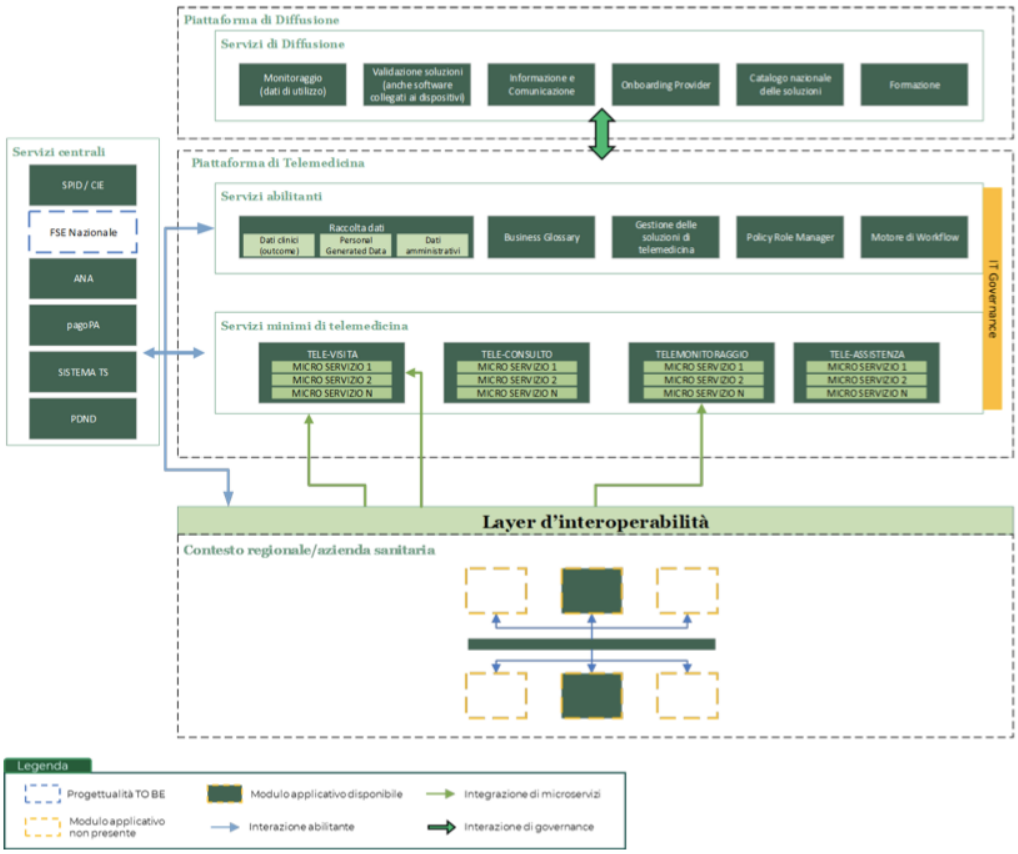


Figura 1

L'ottica è quella della valorizzazione di quanto **disponibile nel panorama dei contesti locali.** Coerentemente con questi principi, la Piattaforma non impone vincoli di alcun tipo alle soluzioni già presenti nei sistemi regionali, ma, piuttosto, deve rappresentare un ambiente orientato alla integrazione ed interoperabilità. Per raggiungere l'obiettivo, tutte le soluzioni di telemedicina regionali sviluppate, o attualmente in sviluppo, devono sottoporsi ad un processo di validazione. Si deve prevedere che tale processo sia attuato in maniera asincrona e disaccoppiata dall'erogazione del servizio in un ambiente tecnologico di *test* e deve riguardare i moduli previsti nell'architettura, inclusa l'integrazione con il Fascicolo Sanitario Elettronico (e, successivamente, il FSE 2.0) e con i servizi centrali (SPID/CIE, PagoPA, ecc.). Sia la infrastruttura tecnologica, che le risorse professionali necessarie a svolgere tale processo di validazione dell'integrazione devono essere parte della PNT ed essere incluse nei servizi abilitanti forniti dalla Piattaforma e nei relativi canoni previsti dal PEF.

L'approccio a macro-funzioni a livello logico fornisce l'ambiente **capace di adattarsi in maniera incrementale e flessibile rispetto alle esigenze e alle risorse dei diversi contesti locali**.

L'Avviso e l'Allegato prevedono un piano di adozione dei servizi basato sulla fattibilità tecnica e la sostenibilità sul medio lungo periodo. Per ottenere tale obiettivo, si prevede **un percorso di dispiegamento**, che opera **seguendo una logica modulare, multilivello tra i servizi presenti e sviluppati a livello nazionale e la relativa integrazione con quanto disponibile, o estendibile, nel contesto locale** e nazionale. In questa logica, è fondamentale che **le Regioni/Aziende Sanitarie ("AASS") provvedano alla progressiva integrazione con i servizi centrali e con lo strato (*layer*) dei servizi abilitanti erogati a livello nazionale.** In questo approccio, risulta di fondamentale importanza **l'adozione di un sistema comune di codifiche mediante l'utilizzo di un *Business Glossary*** uniforme, che faciliterà ed abiliterà l'integrazione (cfr. figura 1).

La PNT, inoltre, come richiesto nell'Avviso e nell'Allegato, deve essere in grado di sviluppare le **integrazioni con i sistemi centrali dispiegati a livello nazionale previsti per il processo di transizione digitale dei servizi erogati dalla pubblica amministrazione (la "PA")**. Pertanto, la PNT deve integrarsi con il Sistema Pubblico Identità Digitale ("**SPID**")/Carta d'Identità Elettronica ("**CIE**"), il Fascicolo Sanitario Elettronico Nazionale ("**FSE**"), l'Anagrafe Nazionale Assistiti ("**ANA**"), il sistema "**PagoPA**", il Sistema Tessera Sanitaria ("**Sistema TS**"), la Piattaforma Digitale Nazionale Dati ("**PDND**").

Ne consegue che i **servizi abilitanti rappresentano un insieme delle migliori pratiche organizzative e di processo, alle quali possono essere associate delle componenti applicative che ne favoriscono l'adozione/fruizione da parte dei contesti locali**. Pertanto, come da indicazioni metodologiche dell'Avviso e relativo Allegato, il PTAS mira a consentire che tali servizi siano in grado di realizzare **uno strato abilitante l'efficientamento e l'omogeneizzazione di nomenclature, tassonomie, codifiche, nonché gestire, in maniera coerente e puntuale, la componente organizzativa per coordinare la varietà di attori coinvolti nelle diverse *use case***. Ciò comporta che la Piattaforma debba presentare delle soluzioni che le consentano di essere adattativa alle nuove esigenze che, via via, dovessero essere manifestate dagli attori coinvolti o dalle amministrazioni (sia quella centrale, che quelle regionali) in fase di esecuzione del contratto di concessione (la "**Concessione**").

Relativamente al modello architetturale, come indicato nell'Avviso e nell'Allegato, si prevede un ambiente totalmente *cloud* - in conformità al principio "*cloud first*", che permea le iniziative di digitalizzazione contemplate nel PNRR - con un ambito nazionale, *i.e.* servizi abilitanti a livello centrale.

L'infrastruttura di erogazione della PNT prevede la realizzazione di un nodo centrale, che, nel caso sia necessario, può prevedere più istanze.

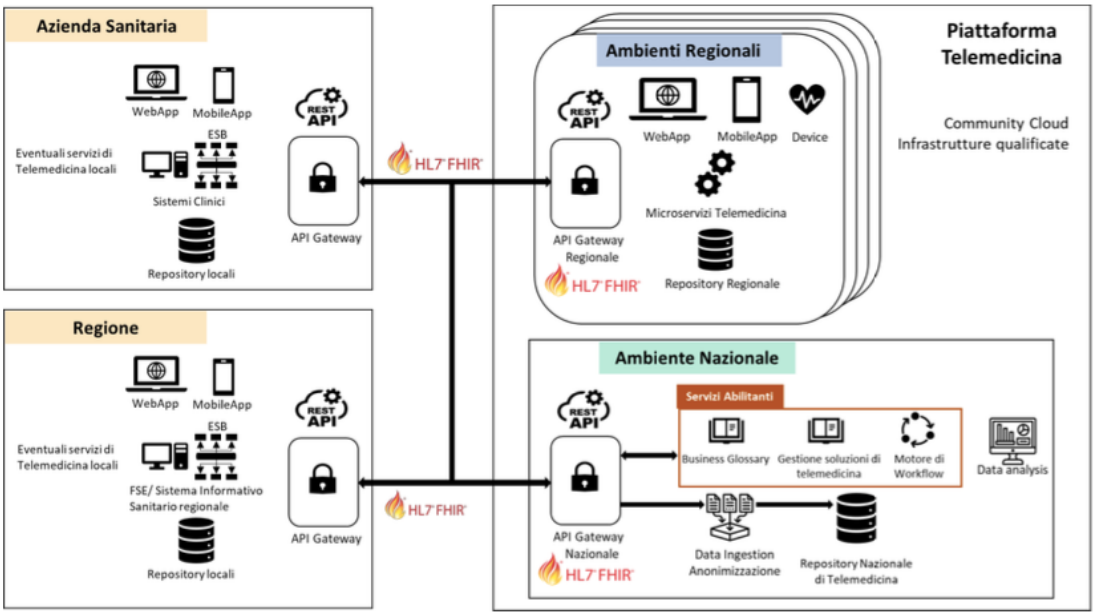


Figura 2

La interoperabilità è garantita a tutti i livelli da ***API Gateway*** (*standard* HL7/FHIR), **abilitanti la gestione e lo scambio di dati e documenti strutturati attraverso l'esposizione di *API REST*** (*framework* di sicurezza OAuth 2.0, utilizzo di un canale criptato). Tali *API Gateway* HL7/FHIR, inoltre, sono **componenti comuni, condivise con l'architettura applicativa del FSE 2.0** e con l'Ecosistema dei Dati Sanitari ("**EDS**"), come descritto dal documento "***Piattaforma di Telemedicina ed Ecosistema FSE - Punti di contatto e raccordo tra i due progetti***", predisposto dal Ministero della Salute, dal Dipartimento per la trasformazione digitale e da AGENAS, che riassume i punti di contatto e di raccordo tra i due progetti.

Per essere in linea con le aspettative nazionali e permettere il corretto uso delle risorse, il Concessionario deve progettare ed eseguire la PNT di concerto con tutti gli attori coinvolti, come meglio specificato nel capitolo 7 del PTAS, in modo che si tenga conto delle componenti previste dal FSE 2.0, già disponibili, e/o di quelle eventualmente ancora in fase di sviluppo: è necessario, quindi, tenere conto della evoluzione ma, al contempo, rispettare il **termine essenziale** di consegna dell'infrastruttura della Piattaforma entro novembre 2023.

Nel caso in cui talune componenti del FSE non siano rese disponibili, di concento con AGENAS, è possibile attivare il c.d. "*Assetto Transitorio*" come descritto nel capitolo 5 del PTAS.

Questo approccio basato su ***API Gateway*** fa sì che la prospettazione della PNT, così come articolata nel PTAS, si integri **con gli altri componenti dell'ecosistema sanitario regionale,** e supporti **la conversione dei dati *legacy*, o formati HL7-v2/v3 o HL7-CDA, in formato FHIR, secondo i modelli definiti a livello centrale.**

In linea con l'architettura prevista nelle indicazioni metodologiche di cui all'Allegato (riportata in figura 2), la Piattaforma adotta un approccio **"*event-driven*"**: quest'impostazione **consente la comunicazione in "*near real-time*"** tra i micro-servizi a livello regionale e nazionale, **al fine di abilitare la diffusione del patrimonio informativo associato agli eventi registrati nei diversi sistemi informativi**. Tali eventi e dati sono, poi, analizzati grazie ai cruscotti previsti, come strumento di controllo e monitoraggio, nella PNT.

Uno degli elementi determinanti per il successo dell'intervento oggetto del PTAS è lo strato d'interoperabilità che permette **una collaborazione applicativa dei verticali regionali e aziendali verso i micro-servizi della PNT**, che deve garantire **l'orchestrazione nei contesti locali e la corretta fruizione di dati e servizi da - e verso il - livello centrale.** L'integrazione delle componenti applicative nella Piattaforma segue una ***roadmap* di evoluzione tecnologica incrementale:** tale approccio abilita **la corretta gestione**, da un lato, **delle complessità implementative** e, dall'altro, dei **relativi impatti sui rispettivi portafogli applicativi locali**, che, quindi, devono prevedere l'aggancio alla PNT, con il fine di garantire gli obiettivi fissati da AGENAS.

La Piattaforma, di cui al PTAS, deve far uso e riferirsi a ***standard* definiti a livello nazionale**, così da raggiungere gli obiettivi **di *performance* in termini di scalabilità e di robustezza dei canali di comunicazione**, nonché abilitare

l'interoperabilità tra le Regioni per la condivisione delle informazioni e dati dei pazienti, in pieno ossequio alle normative vigenti.

La PNT è concepita con quanto previsto nella nuova architettura FSE 2.0, basata su *standard* HL7/FHIR e quindi deve essere perfettamente aderente a quanto descritto dalla Linee Guida per l'Attuazione del Fascicolo Sanitario Elettronico, pubblicate in G.U. n. 160 del 11/07/2022.

Relativamente alla integrazione tecnica con i dispositivi medici, e non, presenti sul mercato, la PNT, di cui al PTAS, deve essere strutturata in modo da essere in linea con lo *standard* ISO/IEEE 11073 SDC ed i profili IHE del dominio PCD (già *standard* Continua), introducendo anche le parti di HL7/FHIR, come definite dal progetto GEMINI.

Inoltre, la Piattaforma deve essere in grado di offrire tre livelli di integrazione, che concorrono a delineare lo scenario tecnologico con cui i moduli della Piattaforma sono innestati all'interno del contesto locale (regionale e delle singole AASS), segnatamente: integrazione tramite SDK; integrazione tramite API (*API first*); utilizzo moduli della Piattaforma.

I servizi abilitanti offerti nell'ambito della Piattaforma devono mettere a disposizione le componenti applicative che permettano di realizzare le migliori pratiche organizzative e di processo afferenti alle soluzioni di telemedicina. (Figura 3 è la descrizione di alto livello dello *stack* architetturale afferente all'Istanza della PNT, in linea con quanto ipotizzato nell'Allegato).

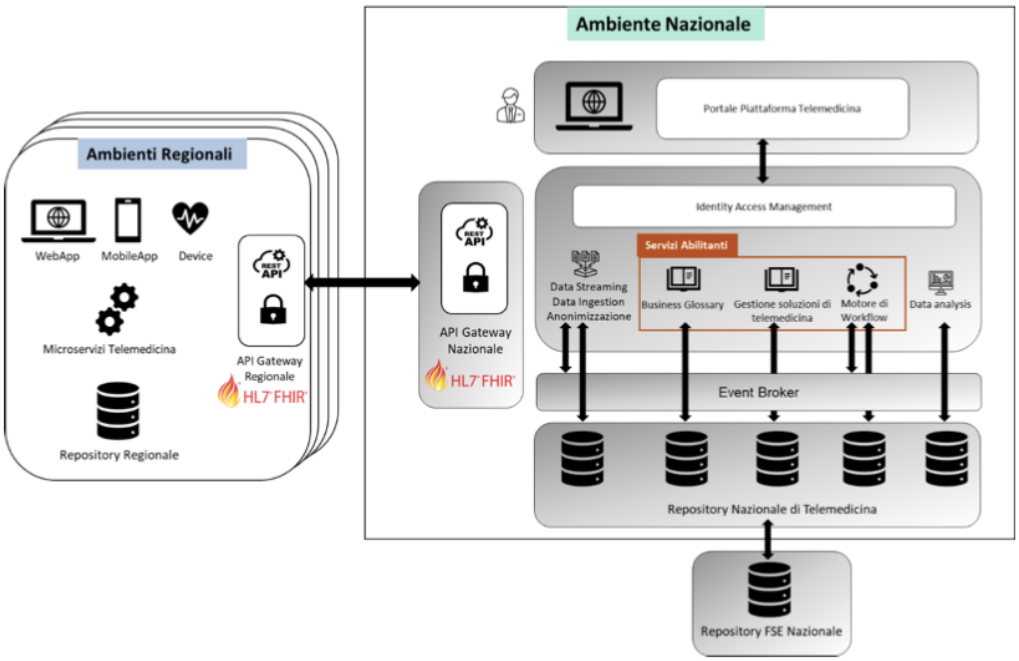


Figura 3

Per garantire il **governo della PNT ed il monitoraggio della corretta esecuzione delle relative prestazioni**, il PTAS compendia un *middleware* per la gestione delle logiche operazionali sui dati e la creazione di cruscotti di analisi, uno strato per la gestione degli eventi e uno strato di persistenza di dati anonimizzati e raggruppati di tutte le Regioni.

Come già accennato, le caratteristiche dell'architettura della PNT devono essere in grado di supportare l'implementazione sia di un *repository* nazionale di Telemedicina, che l'uso dell'EDS e del *Gateway* previsti nel FSE 2.0, per consentire il raggiungimento dell'obiettivo di rendere diffuso ed uniforme, sul territorio nazionale, l'utilizzo e l'alimentazione del FSE stesso, in una logica di riuso e per garantire, al contempo, il raggiungimento degli obiettivi relativi al PNRR, tra cui l'avvio della PNT entro novembre 2023. Tale approccio è in linea con l'eventuale attivazione del c.d. "*Assetto Transitorio*", che sarebbe realizzato (nel caso di attivazione da parte di AGENAS) secondo le linee guida e di concerto con tutti gli attori coinvolti nella sua realizzazione.

Nella progettazione della PNT deve essere garantita **la scalabilità orizzontale** e prevista **la classificazione dei dati ricevuti secondo la categorizzazione**

indicata nel modello logico funzionale, prevedendone l'elaborazione di risorse FHIR.

È prevista l'attivazione di un archivio dell'*event broker* ("*near real-time event-streaming database*") e, inoltre, devono essere elaborati ed aggiornati i cruscotti di analisi definiti (*i.e. outcome* clinici, dati operativi di utilizzo, ecc.), chiavi ed indici per accesso veloce al dato, sia mediante tecniche tradizionali, che attraverso approcci innovativi basati su *machine learning* ("ML") e intelligenza artificiale ("AI").

Una componente fondamentale - ed al tempo stesso critica - della Piattaforma è il motore di *workflow*, che consente all'ambiente nazionale di disegnare dei processi/flussi operazionali che sono eseguiti anche in funzione degli eventi ricevuti dagli ambienti regionali. Tale *workflow* è in grado di adattarsi alle informazioni che, via via, riceve e, in ogni caso, ha la capacità di adeguarsi facilmente (flessibilità) alle eventuali mutate esigenze che possano scaturire durate l'esecuzione della Concessione. A tal fine, devono essere previsti, per ogni componente funzionale, degli *hook* (agganci), che permettano al *workflow* di attivare le singole istanze.

L'Avviso e l'Allegato prevedono che la PNT contempli la possibilità, per i Servizi minimi di Telemedicina, di accedere ai dati standardizzati a livello centrale, quali dispositivi medici, metriche di monitoraggio, il *Business Glossary* e i *template* HL7/FHIR, definiti per la messa a disposizione delle codifiche e PDTA, il trasporto dei dati ed interoperabilità con i sistemi in essere regionali e delle AASS.

Il sistema *IAM* (*Identity Access Management*) contempla una integrazione con i sistemi locali di Regione/AASS di autenticazione basata su *SAML/OAuth* 2.0, così da garantire un adeguato livello di sicurezza nei contesti locali e la sua realizzazione deve assicurare, sempre, un meccanismo di autenticazione a due fattori.

Tutti i servizi concorrono ad alimentare il patrimonio informativo relativo dei dati di utilizzo delle soluzioni di telemedicina: tale informazione è da collezionare a livello centrale per dare evidenza dei risultati e della diffusione della PNT.

In tale logica, la componente "*event broker*" rappresenta il canale di comunicazione tra i micro-servizi e consente di gestire la consistenza eventuale del dato in un ambito di transazioni distribuite.

I *driver* tecnologici, che rappresentano i requisiti non funzionali propedeutici per la progettazione della Piattaforma, considerati per la stesura del PTAS fanno riferimento a quelli contenuti all'interno del Piano Triennale per l'informatica nella PA redatto da AGID (il "Piano AGID"), segnatamente: *Digital&mobile first*; *Digital identity only* (SPID e CIE); *Cloud first* (atto a prevenire il rischio di *lock-in*); Interoperabile *by design*; Sicurezza e *privacy by design*; *User-centric*, *data-driven* e agile; *Open source*.

Sempre in base al Piano AGID, i *driver* tecnologici, utilizzati per la soluzione progettuale sono: *Cloud Readiness*; Architettura a micro-servizi; Containerizzazione; *Mobile Oriented*; Sicurezza; Autenticazione e Autorizzazione; *Privacy* e *Compliance GDPR*; Usabilità e Accessibilità; Flessibilità ed Estendibilità; Scalabilità; Disponibilità.

La soluzione tecnologica di cui al PTAS è ideata in coerenza con il documento del Ministero per la Transizione Digitale denominato *Strategia Cloud Italia*.

In particolare, i servizi Cloud erogati per la PNT sono adottati in modo regolamentato, al fine di mitigare i rischi sistemici dell'adozione del *Cloud*.

In linea con le disposizioni applicabili in questo contesto, **i dati sanitari dei cittadini sono classificati come critici,** mentre i **dati e servizi relativi a portali istituzionali delle amministrazioni sono classificati come ordinari.**

Bisogna tenere presente che i dati e servizi sono classificati in base al danno che una loro compromissione, in termini di confidenzialità, integrità e disponibilità, provocherebbe al sistema Paese. I dati e servizi sono, dunque, suddivisi nelle seguenti classi:

- Strategici: dati e servizi la cui compromissione può avere un impatto sulla sicurezza nazionale;
- Critici: dati e servizi la cui compromissione potrebbe determinare un pregiudizio al mantenimento di funzioni rilevanti per la società, la salute, la sicurezza e il benessere economico e sociale del Paese;
- Ordinari: dati e servizi la cui compromissione non provochi l'interruzione di servizi dello Stato o, comunque, un pregiudizio per il benessere economico e sociale del Paese.

In accordo alla strategia del governo e alla classificazione di dati e servizi, i servizi *Cloud* qualificati identificati per la PNT sono erogati in linea con i seguenti vincoli:

- *Cloud* Pubblico Qualificato e Pubblico Criptato, ospitano i dati e servizi ordinari (portali informativi e dati non sanitari dei cittadini);
- *Cloud* Pubblico Criptato, Privato/Ibrido "su licenza" e Privato Qualificato potranno ospitare dati e servizi critici (dati sanitari dei cittadini).

Nel caso della PNT, si esclude l'uso del *Cloud* Privato Qualificato, che appare maggiormente orientato verso la gestione, esclusivamente, dei dati strategici.

Le prescrizioni e i principi trasversali del PNRR permeano l'intera congetturazione del PTAS, sia sotto il profilo tecnico, sia dal punto di vista prestazionale e, di conseguenza, contrattuale, così da contribuire ad un percorso di transizione ecologica verso soluzioni *carbon neutral* o anche *carbon free*.

La Piattaforma deve essere progettata, realizzata e, infine, gestita secondo il principio del *Do Not Significant Harm* ("DNSH"), ossia in modo da non arrecare un danno significativo all'ambiente.

Per tale obiettivo, è necessario garantire elevatissima efficienza energetica e prevedere l'uso di energia prodotta da fonti rinnovabili.

Per dimostrare l'impronta ambientale, la PNT deve prevedere l'uso di sistemi per il calcolo del *carbon footprint*, verificato e validato. Tale approccio deve consentire sia il calcolo degli impatti strettamente e direttamente connessi con le proprie attività, che quelli legati all'utilizzo, da parte degli utenti, di servizi di telemedicina (indiretti).

Per la stessa natura del progetto, il TAG DIGITALE è maggioritario.

2. Piattaforma Nazionale di Telemedicina – PNT

2.1. Principi Base

L'impostazione architetturale per la soluzione prescelta deve far riferimento ai seguenti principi di base, che sono strettamente coerenti con il Piano AGID. Tali principi sono, dunque, tenuti in considerazione in tutti i paragrafi di cui al presente capitolo 3 del PTAS e, in particolare, nella realizzazione delle singole componenti/moduli.

Principio di Indipendenza: ciascun modulo deve poter funzionare in modo auto-consistente, minimizzando le dipendenze dagli altri moduli facenti parte della soluzione. Inoltre, deve farlo impiegando tecnologie e strumenti che non costituiscano un vincolo nei confronti di un singolo o ristretto gruppo di fornitori di mercato, evitando il c.d. fenomeno del "*Vendor Lock In*". Tale strategia deve essere realizzata, preferibilmente, mediante l'adozione di tecnologie *open source* per l'implementazione delle nuove componenti. Nel caso di utilizzo di prodotti di mercato, le componenti oggetto di fornitura devono garantire la *compliance* con gli *standard* internazionali di interoperabilità sia nelle modalità di interazione con tutto il resto dell'architettura, sia nella generazione e persistenza dei dati. In ogni caso l'intera architettura dovrà essere costituita da componenti sia di nuova realizzazione, che da prodotti di mercato, che da componenti *open source* dove la persistenza e la modalità di interazione siano basate su *standard* FHIR nelle varie specifiche declinazione per le funzionalità risolte da tale componente; più in generale ogni componente dell'architettura deve essere sostituibile con soluzioni analoghe o disponibili sul mercato o realizzabili *ex novo* grazie all'aderenza *by design* gli *standard* FHIR e/o agli *standard* di mercato di persistenza di dati e regole.

Principio di Flessibilità, Robustezza, Scalabilità e Riuso: tali caratteristiche sono declinate come segue:

- flessibilità: le funzionalità offerte devono godere di capacità di adeguarsi con flessibilità al contesto in cui vengono rese disponibili,
- scalabilità: i moduli funzionali devono scalare sia verticalmente (variazione del carico sostenuto), che orizzontalmente (istanze disponibili e loro collocazione geografica),

- robustezza: i moduli funzionali devono essere in grado di far fronte a condizioni di elevato *stress* tecnico senza presentare cedimenti o condizioni di errore che ne impediscano l'uso,
- riuso: i moduli devono essere intercambiabili e, quindi, adatti ad essere riusati in altri contesti o ad essere sostituiti da altri che provengano da iniziative nazionali che sono, per loro natura, integrate con la PNT.

Principio di Interoperabilità: ciascun modulo funzionale deve avere come via preferenziale di accesso alle sue funzioni l'interazione a servizi con gli altri moduli o moduli esterni alla PNT. Questo principio si sostanzia mediante:

- l'impiego di *standard* internazionali, nazionali o regionali di interoperabilità per la realizzazione di tutte le funzionalità di interazione tra moduli,
- l'impiego di API basate sul paradigma RESTful API, così da offrire un'interfaccia a servizi leggera, semplice, facilmente accessibile da qualsiasi contesto (es: *desktop*, *mobile*, *server*, ecc.).

Principio di *Data Protection*: il sistema deve adottare il paradigma della *Privacy by Design and Default*, garantendo che l'insieme dei dati gestito/visualizzato sia esclusivamente quello necessario alla completa esecuzione del processo.

Principio *Cloud First*: il sistema deve essere completamente dispiegabile in ambiente *cloud*, massimizzando l'utilizzo di servizi di Piattaforma, piuttosto che l'installazione di soluzioni infrastrutturali.

2.2. Architettura Funzionale/Applicativa

Il presente paragrafo descrive l'architettura logica della PNT.

2.2.1. Architettura Funzionale Generale

L'architettura funzionale della Piattaforma deve prevedere cinque *layer* logici distinti:

- *Layer* Accesso *Front End*: costituisce il punto di accesso ai servizi della soluzione adottata, attraverso cui gli utenti possono fruire delle funzionalità offerte;
- *Layer* Servizi: rappresenta lo strato in cui sono collocate le applicazioni, contenenti la logica di *business* del sistema e fruibili mediante API. Per

alcuni di questi servizi è disponibile, in aggiunta all'accesso attraverso API, l'esperienza d'uso mediante un'interfaccia utente semplice e ottimizzata per classe di utenza;
- *Layer* Orchestrazione: rappresenta l'area i cui moduli governano la costituzione e l'avanzamento dei processi di lavoro, siano essi di natura clinico-diagnostica, sanitaria, o amministrativa;
- *Layer* Interoperabilità: rappresenta lo strato di gestione delle interazioni tra i moduli funzionali della Piattaforma ed i sistemi terzi;
- *Layer* Dati: rappresenta l'impianto di gestione dei dati.

La Piattaforma deve, inoltre, essere in grado di offrire tre modalità di integrazione, che concorrono a delineare lo scenario tecnologico con cui i moduli sono innestati all'interno del contesto locale (regionale e delle singole AASS), segnatamente: integrazione tramite SDK; integrazione tramite API (*API first*); utilizzo moduli della Piattaforma.

L'accesso mediante le prime due modalità avviene attraverso il *Layer* Interoperabilità, mentre l'accesso mediante l'utilizzo moduli della Piattaforma (passaggio di contesto) avviene attraverso il *Layer* Accesso *Front End*.

Questa differenziazione si rende necessaria in virtù delle caratteristiche degli *stream* di dati che le suddette modalità impiegano, ossia, rispettivamente dati grezzi (ad es. risorse FHIR in JSON), nelle prime due modalità, e dati interpretabili da un *browser* (es. pagine HTML, comandi http), nella terza modalità.

Sia il *Layer* Interoperabilità, che il *Layer* Accesso *Front End* interagiscono con i moduli del *Layer* Sicurezza per verificare credenziali e diritti di accesso dell'utente.

L'architettura deve essere integrabile con il *Gateway* nazionale ("GW") e l'EDS, come previsto dal FSE 2.0, in ottica di riuso, garantendo, al contempo, i livelli di servizio e gli obiettivi specifici della PNT.

Il seguente diagramma riassume l'architettura funzionale della Piattaforma:

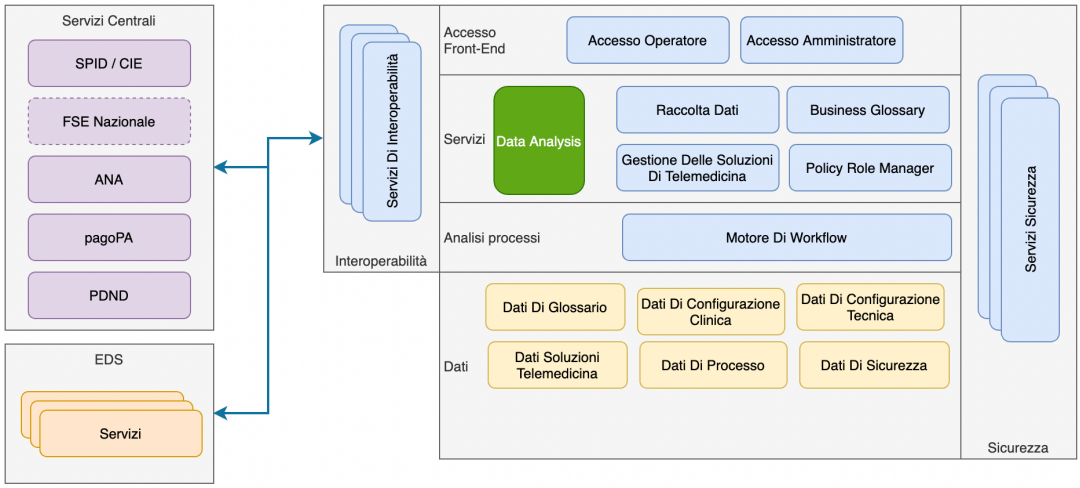


Figura 4: Architettura Funzionale della soluzione

Ciascuna delle componenti funzionali deve essere dotata delle seguenti caratteristiche, in modo uniforme rispetto all'intera soluzione adottata:

- uniformità del *Design System*: l'aspetto grafico degli elementi di interfaccia utente, la disposizione ed il comportamento degli elementi stessi, le icone impiegate, le *palette* di colori e le caratteristiche di accessibilità devono essere uniformi. Tutti gli elementi devono concorrere ad esporre una interfaccia semplice ed intuitiva in cui gli elementi devono essere riconoscibili e ben codificati in termini di forme e colori. Per raggiungere questo obiettivo, viene definito uno U-KIT grafico (sia per mobile che per il *web*) condiviso ed usato per tutti i *Front End* di tutti i moduli;
- fruibilità da dispositivi mobili: tutte le funzionalità esposte dalle componenti devono essere fruibili a partire da dispositivi mobili. In particolare:
  - quando si tratta di funzionalità esposte mediante interfacce utente, queste devono essere automaticamente adattate, così da consentire una fruibilità da dispositivo mobile;
  - quando si tratta di funzionalità a servizi, tali servizi devono essere esposti mediante *standard* che siano predisposti per la fruizione da parte di dispositivi mobili, ad es., API REST.

2.2.2. Architettura Applicativa

L'architettura applicativa della PNT deve essere realizzata adottando un paradigma di "*Service Oriented Architecture*" ("SOA"), in cui ciascuna componente applicativa è costituita da un'aggregazione di micro-servizi.

L'architettura deve prevedere la realizzazione di un articolato ecosistema di micro-servizi ad alto livello di coesione ed a basso livello di accoppiamento.

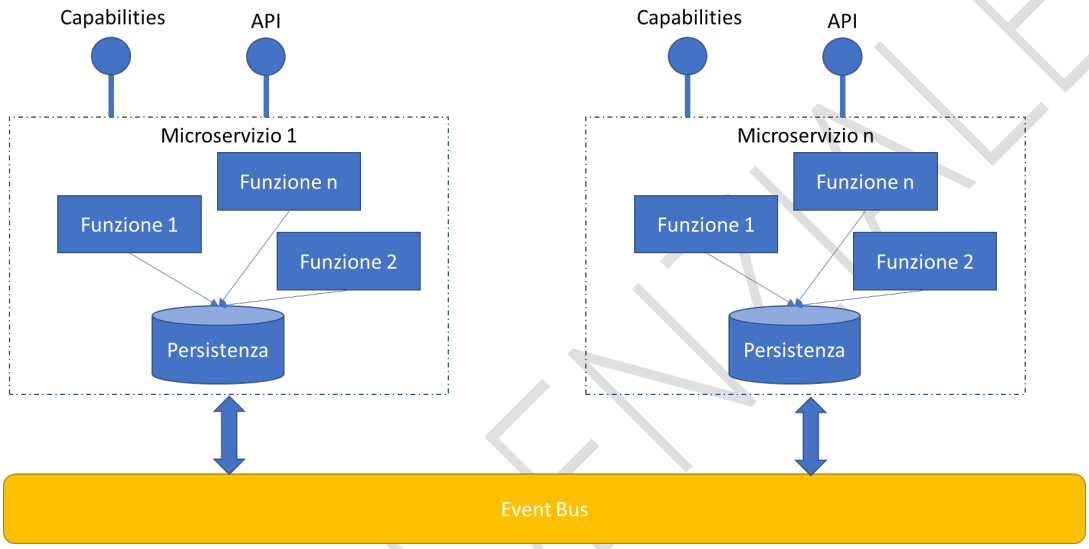


Figura 5: Esempio di Architettura a Micro-servizi prevista

2.2.2.1. Caratteristiche dei Micro-servizi

Ciascuno dei micro-servizi che costituiscono l'architettura applicativa deve essere caratterizzato da quanto segue:

1. indipendenza di sviluppo: il ciclo di vita di sviluppo, rilascio e manutenzione della componente deve essere indipendente da quello delle altre componenti con cui essa è chiamata ad interagire;
2. alta coesione: ciascun micro-servizio deve essere indipendente nella gestione del proprio segmento di dominio, accedendo, in maniera esclusiva, alle proprie sorgenti dati. L'utilizzo di paradigmi come il *bounded context* e l'*aggregate pattern* deve agevolare la scomposizione del sistema in elementi autoconsistenti ad elevato grado di coesione, consentendo il governo dei punti di contatto;
3. basso livello di accoppiamento: la dipendenza tra i veri micro-servizi deve limitarsi alla realizzazione di funzioni che escono dalla propria sfera di competenza, prevedendo, quindi, a titolo esemplificativo:
   a. integrazione con il sistema di *workflow*;

   b. gestione dei consensi e delle *policy* di accesso;
   c. accesso a funzionalità e informazioni esterne al proprio contesto funzionale;
   d. gestione di eventi;
   e. integrazioni limitate strettamente ad aspetti tecnici;
4. emissione proattiva di eventi: in maniera assolutamente proattiva, ciascun micro-servizio pubblica eventi di particolare rilevanza su un *event bus*, allo scopo di incrementare la flessibilità del sistema; tali eventi possono attivare diverse azioni sul sistema, senza che questo sia programmaticamente già pianificato;
5. standardizzazione nell'emissione dei *log*: ciascun micro-servizio deve emettere *log* applicativi per consentire la tracciatura completa delle transazioni. Per questa componente, è necessario optare per soluzioni basate su codice aperto, che sono caratterizzate da una definizione chiara della semantica e della sintassi nell'erogazione del *log* (es. *OpenTemeletry*, *OpenTracing*);
6. API di *Capabilities* - Esposizione: ciascuna componente deve esporre l'insieme di funzionalità che è in grado di erogare, in base alla propria maturità di sviluppo ed alle caratteristiche di configurazione di ciascuna sua istanza. Ad es., l'API indica se parte delle funzionalità supportate dalla componente sono non disponibili oppure disattivate su una sua istanza, poiché non utili nello specifico contesto d'uso. L'API di *Capabilities* esposta deve essere uniforme in ciascuna componente della soluzione: essa avrà un'unica specifica tecnica e una semantica uniforme dei dati scambiati;
7. API di *Capabilities* – Consumo: ciascuna componente della soluzione deve interagire con le altre componenti, verificandone, preventivamente, le *capabilities* mediante la relativa API esposta. In virtù dei dati ottenuti in risposta, la componente deve adeguare il proprio comportamento nel realizzare l'interazione: ad esempio, deve evitare di trasferire dati che un componente ricevente non è in grado di impiegare, o non è configurato per farlo;
8. *design stateless*: ciascuna componente deve essere progettata in modo da non dipendere da un proprio stato interno per erogare i servizi;
9. separazione delle responsabilità tra *layer* applicativi: la componente deve separare l'implementazione dell'interfaccia utente dalla logica di *business* e persistenza delle informazioni.

L'insieme di queste caratteristiche enfatizza la capacità del sistema di essere indipendente dal singolo *vendor*, evitando, così, il rischio di *lock-in*.

2.2.2.2. Caratteristiche di Interoperabilità

In un'architettura basata sui micro-servizi, riveste particolare importanza la comunicazione che avviene tra essi. Nelle indicazioni metodologiche di cui all'Allegato è descritto che *la componente "event broker" è il "canale di comunicazione tra i micro-servizi, per gestire la consistenza eventuale del dato in un ambito di transazioni distribuite"*.
L'architettura complessiva, quindi, deve rispettare i paradigmi dell'*Event-Driven Architecture* secondo i seguenti requisiti:

1. la comunicazione fra i micro-servizi deve essere asincrona nella quasi totalità dei casi. Possono fare eccezione le comunicazioni puntuali per l'accesso a specifiche informazioni (*get by id*) basate su protocollo HTTP/S;
2. la componente "*event broker*" è il canale di comunicazione tra i micro-servizi, per gestire la consistenza finale del dato in un ambito di transazioni distribuite;
3. l'archivio dell'*event broker* deve essere composto da un "*near real-time event-streaming database*" che combina lo *stream* dei dati con un modello di *database* relazionale utilizzando la sintassi SQL;
4. la comunicazione fra i micro-servizi deve seguire un approccio basato sull'utilizzo degli *standard* secondo un ordine di priorità:
    a. ove possibile si utilizzano *standard* internazionali quali HL7-FHIR, XACML, ecc.,
    b. ove non è possibile utilizzare uno *standard* internazionale, deve appoggiarsi a *standard de facto*,
    c. in ultima istanza, deve definire meta-modelli chiari con sintassi e semantica prescrittiva.
5. La persistenza dei dati che sono oggetti di scambio tra le varie componenti applicative deve essere basata su modelli *standard* FHIR e/o su modelli dati basati su *standard* internazionali di riferimento in ambito clinico-sanitario, tenendo conto delle disposizioni in ambito EHDS.

L'insieme di queste caratteristiche enfatizza la capacità del sistema di essere indipendente dal singolo *vendor*, evitando così il rischio di *lock-in*, e, al contempo, di essere pronto alle integrazioni verso le altre iniziative nazionali.

2.2.2.3. Altre Caratteristiche

Le singole componenti applicative devono prevedere, tra le loro API, uno, o più, accessi di interoperabilità, che consentano al *Workflow Manager* di richiamarla, quando uno specifico *workflow* ne richiede l'attivazione.

Da un punto di vista di persistenza, ciascuna componente deve persistere i dati impiegando tecnologie di tipo *Relational Database Management System* (RDBMS, ad es: Postgresql) oppure no-sql (ad es: MongoDb, ElasticSearch). **Indipendentemente dalla tecnologia impiegata, non vi deve essere presenza di logica di *business* realizzata mediante tecnologie o linguaggi proprietari, quali, ad es., l'impiego di *stored procedure* SQL.**

2.2.2.4. Caratteristiche di Data Protection

La Piattaforma deve fornire ad AGENAS un supporto nell'attuazione degli adempimenti del GDPR e all'applicazione delle Misure minime di sicurezza ICT AgID per le PA.
L'offerta deve esplicitare le misure proposte per garantire che la fornitura del servizio sia sempre conforme alle norme sulla protezione dei dati, compresa una descrizione delle misure di sicurezza tecnica proposte e delle garanzie per il trattamento dei dati personali.
Ai fini di rispondere ai requisiti di *data protection* ed in termini non esaustivi, la Piattaforma deve prevedere:

- l'applicazione di principi di minimizzazione dei tempi di conservazione dei dati trattati;
- l'applicazione di principi di minimizzazione dei privilegi di accesso;
- processi di classificazione dei dati al fine di identificare i criteri di protezione;
- l'applicazione dei principi di *Privacy* e *Security by Design*;
- l'uso di soluzioni di cifratura dei dati;
- applicazione di criteri di pseudonimizzazione e anonimizzazione;
- l'uso di dati non reali negli ambienti non di produzione.

2.2.2.5. Caratteristiche di Usabilità e Accessibilità

Data la tipologia e disomogeneità degli utenti, la *user experience* riveste un ruolo essenziale per realizzare la Piattaforma in modo che sia utile, usabile ed accessibile. I servizi che compongono l'ecosistema della PNT devono essere fruibili in differenti modalità e attraverso diversi *device*. Le indicazioni metodologiche, inserite nell'Allegato, infatti, richiedono che "*l'interfaccia*

grafica (Front End) della Piattaforma Nazionale di Telemedicina deve essere progettata secondo il paradigma mobile first, cioè a interfacce responsive".
La progettazione e realizzazione della *user experience* deve rispettare sia i principi espressi nel Piano AGID, sia le linee guida di *design* per i servizi *web* della PA.
Tali indicazioni valgono sia per i servizi abilitanti base della PNT, oltre che per quelli opzionali, previsti a listino e, in ogni caso, devono essere rispettati da tutte le applicazioni che devono essere integrate nella PNT.
Nel seguito, sono dettagliati i principali requisiti che devono essere soddisfatti.

User-centric, data driven e agile
Questo principio, espresso nel Piano AGID, richiede di procedere con una progettazione che metta al centro l'esperienza dell'utente, semplificando la navigazione attraverso paradigmi noti e costantemente aggiornati rispetto all'evoluzione delle interfacce. Nella realizzazione, è richiesto un approccio basato sui principi della *Lean UX* e di tipo "*User-centered Design*".

Usabilità e accessibilità
La Piattaforma deve rispondere ai requisiti di accessibilità e usabilità identificati da AGID all'interno delle Linee guida di *design* per i servizi digitali della PA. La Piattaforma deve costituire un *asset* digitale che abiliti l'inclusione sociale dei soggetti che la utilizzano.
Lo sviluppo dell'interfaccia grafica deve seguire e aderire ai seguenti principi guida:

1. intellegibilità: l'interfaccia deve esporre in maniera chiara, semplice e pulita le funzionalità offerte all'utente, in termini di:
    a. contesto visuale, utilizzando un appropriato linguaggio grafico e testuale che sia omogeneo e consistente nell'ambito dell'intero sistema;
    b. interazioni, laddove la disposizione e l'aspetto degli oggetti di interazione devono rendere chiara all'utente l'azione e gli effetti che ne conseguono;
    c. architettura delle informazioni, la quale deve garantire la presentazione comprensibile, esaustiva ma essenziale delle informazioni e dei dati;
2. facilità di apprendimento: l'interfaccia deve minimizzare lo sforzo cognitivo da parte dell'utente per impararne le funzionalità;
3. accessibilità: l'interfaccia deve facilitare l'accesso a tutte le funzionalità offerte, indipendentemente da eventuali disabilità dell'utente. La Piattaforma deve rispondere in maniera puntuale a quanto definito da

AGID all'interno delle linee guida sull'accessibilità degli strumenti informatici, le quali riportano quanto descritto nell'articolo 11 della legge 9 gennaio 2004, n. 4 e ss.mm.ii., recante "*Disposizioni per favorire e semplificare l'accesso degli utenti e, in particolare, delle persone con disabilità agli strumenti informatici*" (la "Legge 4/2004") e referenziano la norma UNI EN 301549:2018 che identifica gli *standard* applicabili a livello europeo;

4. produttività: l'interfaccia deve essere realizzata in modo da massimizzare l'efficienza dell'operatore, e deve essere progettata secondo criteri di usabilità centrati sull'utente. A tal fine, deve essere progettata e realizzata in maniera tale da snellire e guidare il lavoro di chi utilizza il sistema.

Uniformità nella navigazione

La PNT deve garantire un'uniformità visiva e di navigazione, indipendentemente dai *device* che sono utilizzati. Mutuando i concetti dell'identità visiva, la PNT deve garantire un'esperienza utente uniforme, sia dal punto di vista della grafica (tipografia, colori, ecc.), sia delle metafore navigazionali, sia dell'infografica.

La PNT deve essere costruita raggruppando le funzionalità di cui all'Architettura Funzionale, delineata sub 3.2.1 del presente capitolo 3 del PTAS, in un unico "pacchetto" logico, che viene definito Nucleo Centrale.

Questa componente centrale è quella che, integrandosi con l'EDS, in modalità bidirezionale garantirà tutti i servizi richiesti dalla PNT

2.2.2.6. Ambito Nazionale

L'ambito nazionale costituisce un esempio di federazione orizzontale: esso, infatti, è costituito dalla distribuzione di una, o più, istanze a livello nazionale (*multi-tenant*), dove, a ciascuna istanza del Nodo nazionale, è attribuita una diversa responsabilità di *governance* e/o operativa.
Ciascun offerente deve indicare, in sede di offerta, quanti Nodi costituiscono l'Ambito Nazionale, considerando la base minima di un singolo Nodo.

2.3. Componenti della PNT

Partendo dal contesto descritto nel PTAS, le componenti della PNT sono:

- Servizi Abilitanti (componenti applicative);
- *Layer* di interoperabilità (componente trasversale);
- *Layer* di Sicurezza (componente trasversale).

Le componenti trasversali, denominate "*Layer* Interoperabilità" e "*Layer* Sicurezza", sono descritte, rispettivamente, nel capitolo 3 e capitolo 4 del PTAS, vista la loro strategicità e peso complessivo, mentre, nei paragrafi che seguono, sono descritte le componenti funzionali che abilitano la PNT secondo gli obiettivi esplicitati dalla Amministrazione.
Il *Layer* Interoperabilità abilita la realizzazione degli obiettivi della PNT. Nella evoluzione della Piattaforma, questo *Layer* deve tenere conto dello sviluppo relativo al FSE 2.0, creando le condizioni di interrelazioni e di riuso dei servizi o di implementazione di nuovi componenti, ove necessario.
Sono stati individuati e descritti, nel paragrafo che segue, i Servizi Abilitanti, ossia quelli facenti parte della infrastruttura centrale della PNT.

Le componenti trasversali, unitamente ai Servizi Abilitanti, devono essere alla base del Piano Economico Finanziario dell'operazione ("PEF").

2.4. Servizi Abilitanti

Nel presente paragrafo sono illustrati i componenti applicativi abilitanti previsti per la PNT che sono:

- *Business Glossary*;
- Gestione Soluzioni di Telemedicina;
- *Policy Role Manager*;
- Motore di *Workflow*;
- Raccolta ed elaborazione dei dati;
- *Data Analytic*.

Le funzionalità che devono essere garantite da ciascun componente sono descritte nei sotto-paragrafi che seguono.
L'insieme costituito dai Servizi Abilitanti, il *Layer* di interoperabilità e il *Layer* Sicurezza devono essere progettati, sviluppati ed installati entro novembre del 2023, per consentire il collaudo della PNT in linea con le previsioni e le richieste dell'Amministrazione.

Nel caso di attivazione di tutto il c.d. "*Assetto Transitorio*" o di parte di esso, lo stesso deve essere progettato per tenere in conto l'evoluzione delle progettualità nazionali, come meglio specificato nel capitolo 5 del PTAS: in ogni caso la sua realizzazione è indipendente, in quanto opzionale, dalle attività relative alla PNT.

2.4.1. Raccolta ed elaborazione dei dati

2.4.1.1. Servizi Raccolta Dati

Il sistema di raccolta dati della Piattaforma è composto da una serie di servizi definiti a livello nazionale atti a gestire tutti i dati e i documenti (tramite riferimento) generati a livello regionale; questa istanza interopera con il sistema FSE nazionale per la gestione dei dati clinici (mediante la sua componente EDS) e *Patient-Generated Data* prodotti nell'ambito della telemedicina ed è la base per l'anonimizzazione e aggregazione dei dati di dettaglio ai fini dell'estrazione di conoscenza (*insight*).

Il diagramma seguente sintetizza l'architettura interna del componente e le sue integrazioni principali con i sistemi nazionali di FSE:

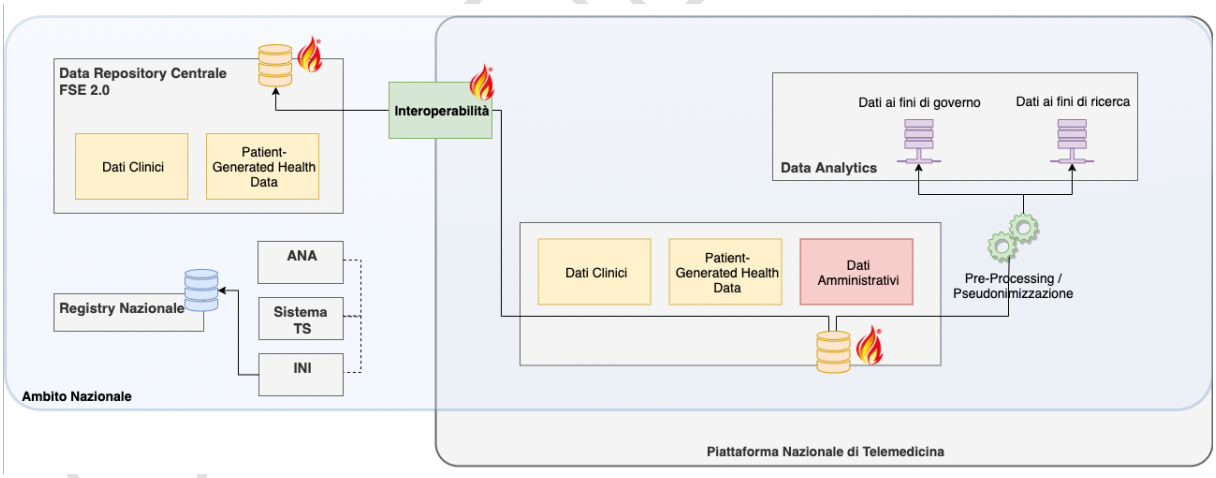


Figura 6: Architettura del Servizio Raccolta Dati

Nel caso in cui, per l'erogazione di un servizio di telemedicina, si acceda a documenti pre-esistenti sul FSE Nazionale, questi saranno utilizzati nell'erogazione del servizio stesso, ma di essi deve essere registrato

solamente il riferimento. Questo riduce al minino la duplicazione/ridondanza dell'informazione, mantenendo la stessa presso l'*owner*.

Un meccanismo analogo deve avvenire anche nell'interazione con gli altri servizi nazionali (ANA, Sistema TS).

Il sistema di raccolta dati della PNT deve rappresentare, quindi, la componente deputata a ricevere, gestire, validare e condividere tutte le informazioni cliniche strutturate (risorse FHIR) e non strutturate (*standard* XDS.b) prodotte dai sistemi di telemedicina ed utili durante il processo, così come i dati amministrativi e quelli direttamente inseriti dai pazienti (*Personal Generated Data*).

Gestione Dati clinici

Di seguito, è riportata una lista, non esaustiva, di alcuni esempi di tipologie di dati clinici, strutturati e non, di pertinenza dei casi d'uso previsti per la telemedicina, segnatamente:

- registrazione video con possibilità di memorizzazione il documento XDS.b a livello locale riferito all'interno di un evento FHIR;
- segni vitali (rilevati tramite dispositivi, classificati come medici certificati, messi a disposizione del paziente) codificati secondo *standard* in linea con le direttive del Ministero della Salute;
- altri parametri clinici rilevati durante il teleconsulto;
- referti/documentazione clinica strutturata o multimediale fornita dagli OOSS o dal paziente (televisita, teleconsulto, telemonitoraggio);
- immagini;
- esito clinico (televisita);
- segnalazioni aggiuntive (es: spontanee);
- informazione clinica paziente-*caregiver*.

In ogni caso, la Piattaforma deve, *by design*, gestire dati clinici strutturati: ossia, dati clinici classificati secondo i nomenclatori definiti dal *Business Glossary*. Quindi, deve essere prioritario operare con i contenuti clinici estratti dai documenti clinici prodotti dai vari applicativi clinico-sanitari; tale codificazione dei dati, necessaria ad eseguire prestazioni cliniche in telemedicina, deve essere ottenuta o tramite la generazione nativa da parte degli applicativi clinici e diagnostici in ambito ospedaliero pubblico e privato e del territorio (MMG, soggetti operativi previsti dal DM77, ecc.) - opzione a tendere preferibile - o tramite l'utilizzo di strumenti di estrazione di tali dati dai documenti presenti negli FSE attuali e/o presenti e generati dal nuovo

FSE.2.0, o utilizzando componenti messe a disposizione nell'Assetto Transitorio e acquisibili nell'elenco dei servizi opzionali.

Personal Generated Data

Nel processo di telemedicina, la parte di acquisizione dei dati clinici significativi del paziente, siano essi inseriti dal paziente stesso o acquisiti dai dispositivi automatici di rilevazione, rappresenta un patrimonio informativo di enorme importanza.

Il servizio ha il compito di rendere fruibile questo patrimonio informativo in un formato che possa, poi, consentire elaborazioni massive ed analisi alla ricerca di *pattern* informativi su classi di pazienti.

Queste le sue principali funzioni:

- API raccolta dati: il servizio espone API capaci di integrare diverse fonti di dati, siano esse strutturate (es. segnali e rilevazioni inviati da dispositivi collegati alla persona), o destrutturate (es. dati raccolti direttamente dal paziente o dal *caregiver*). Tra queste è fonte di primaria importanza l'EDS del Fascicolo Sanitario Nazionale.
- Sistema di arricchimento: prima della loro memorizzazione, i dati sono arricchiti di un insieme di meta-informazioni utili alla loro classificazione e gestione, ottenute tramite applicazione di regole di codifica definite dinamicamente dal servizio stesso o mediante interazione con il *Business Glossary*.
- API per l'accesso ai dati: il modulo espone API per il recupero dei dati clinici tramite le quali tutti gli altri componenti della Piattaforma possono accedere ai dati.

Gestione Dati Amministrativi

La PNT deve consentire di gestire anche informazioni correlate ai processi amministrativi attivati, a fronte dell'erogazione di una prestazione sanitaria in regime di telemedicina, quali, ad esempio: tipo prestazione, esenzione, prenotazione, ecc. In questo modo, si devono attivare componenti specifiche di monitoraggio di indicatori che hanno peso sul governo del servizio dal punto di vista finanziario e, di conseguenza, facilitare, o diversificare, i processi di programmazione strategica nelle scelte di evoluzione della PNT, a fronte dei reali fabbisogni delle amministrazioni utenti (le "PA utenti"), acquisiti dal sistema.

La PNT deve, pertanto, disporre di un modulo specifico di gestione dei dati amministrativi, alimentato automaticamente ad ogni erogazione di una prestazione sanitaria, ed in grado di esporre tali informazioni sotto forma di

flussi di dati opportunamente pseudo-anonimizzati al sistema centrale Nuovo Sistema Informativo Sanitario ("NSIS").
Anche nel caso dei dati amministrativi, il sistema espone delle API capaci di integrare diverse fonti di dati strutturati (sistemi di prenotazione, di prescrizione, di accettazione ambulatoriale, ecc.).

Per conseguire le finalità cui il servizio di raccolta dati mira è fondamentale che il modulo di acquisizione dei dati amministrativi consenta di:

- gestire tutti i dati amministrativi atti ad abilitare il monitoraggio economico finanziario, la programmazione strategica per la gestione ed evoluzione della Piattaforma ed il governo della rete dei servizi sanitari;
- rendere i dati amministrativi raccolti confrontabili con i patrimoni informativi contenuti nelle altre banche dati nazionali;
- inviare i dati al Sistema Centrale NSIS.

2.4.2. *Data Analytic*

La Piattaforma deve mettere a disposizione l'ambiente di "***Data Analytic***", ossia un modulo di memorizzazione (ove necessario per la creazione e la persistenza di cruscotti a servizio di AGENAS), navigazione ed estrazione, centralizzato, dei dati clinici ed amministrativi provenienti dalle diverse fonti al fine di poter avere a disposizione un unico accesso in grado sia di alimentare, per le diverse funzionalità, gli ulteriori servizi previsti dalla Piattaforma, nonché servizi esterni da integrare, sia di offrire uno strumento di consultazione del dato.
Il modello di riferimento per il transito delle informazioni deve prevedere un modello dati estendibile, replicabile e integrato, di risorse FHIR per tutto quanto prescritto dal *framework* FHIR (versione più aggiornata), comprensivo anche di metadati amministrativi e organizzativi, in termini di HR.
Il modulo di "***Data Analytic***" deve fornire, inoltre, servizi API di alimentazione multicanale (http, *code*, ecc.), sulla base di un modello concettuale opportunamente documentato, al fine di poter declinare anche i metadati su risorse FHIR potenzialmente verticalizzate al contesto di riferimento.
La Piattaforma deve esporre un *portfolio* di servizi API per le richieste informative B2B provenienti dall'Amministrazione e da ulteriori potenziali attori invocanti, gestendo sia una multi-rappresentazione degli *output* (HL7 v.2, XML, JSON) sia servizi API per la fornitura *batch* di risorse FHIR tese

all'alimentazione di sistemi di analisi e cruscotti direzionali esterni con un data transfer di grosse quantità di dati (*data-stream*).
La soluzione deve, preferibilmente, basarsi su tecnologie di basi di dati in grado di gestire quantità di dati di grosse dimensioni (*Big Data*).
Avendo accesso, in modo centralizzato, ad una quantità notevole di informazioni, la soluzione deve prevedere un *layer* dedicato alla *Data Analysis che ne consenta la navigazione delle informazioni e l'estrapolazione di "informazioni utili" (es. Data mining) e rendendolo di fatto uno strumento partecipe nei processi decisionali critici*.
Nello specifico il modulo deve essere in grado, al minimo, di garantire la possibilità di:

- gestire l'alimentazione di molteplici *datamart* attraverso i dati provenienti molteplici fonti;
- disporre di uno strumento di consultazione/esplorazione delle informazioni in grado di generare reportistica dinamica, QBE, *cockpit* di controllo, ecc.;
- consentire la profilatura degli utenti, garantendo l'attuazione del cono di visibilità al fine di ottenere una corretta segregazione del dato a seconda dei privilegi (*multi-tenancy*);
- garantire un processo di anonimizzazione e pseudonimizzazione del dato in transito;
- eseguire le fasi di preparazione, trasformazione o filtraggio dei dati;
- rendere disponibile uno strumento in grado di far emergere relazioni, non esplicite, tra i dati;
- eseguire un'estrazione, con tecniche analitiche, di informazione implicita da dati già strutturati, per renderla direttamente utilizzabile;
- eseguire esplorazione ed analisi, eseguita in modo automatico/semiautomatico, su grandi quantità di informazioni al fine di scoprire pattern.

2.4.3. *Business Glossary*

Le attività clinico-sanitarie attuali e future sono improntate all'applicazione della migliore qualità clinica ed al controllo del rischio clinico; tali affermazioni si debbono realizzare in un contesto caratterizzato da una sempre maggiore complessità clinico-operativa dove sia le acuzie. che le cronicità hanno un alto impatto sanitario in un contesto di ottimizzazione delle risorse (sia economiche, che di operatori del settore); in tale scenario, il cambio di paradigma della "*data usability*" è diventato essenziale.

Quattro sono gli elementi che, se combinati insieme, hanno il vantaggio di ridurre il rischio clinico e di supportare al meglio il *clinical pathway* (soprattutto del paziente poli-patologico):

a) collaborazione tra clinici/OOSS. Questo al fine di raccogliere e condividere le migliori pratiche ("EBM") tra le comunità scientifiche in modo "*non invasivo*", ma partecipativo;
b) utilizzo di terminologie e dei sistemi di codifica. Aspetto importante per risolvere il problema delle diverse nomenclature, così da consentire una condivisione totale e significativa delle informazioni cliniche, senza modificare l'approccio operativo quotidiano;
c) presentazione dei dati clinici importanti per quel particolare contesto clinico (*viewer*, *patient synoptic*). Lo scopo è quello di ridurre il quantitativo di informazioni (spesso fuorvianti e che creano dei "*bias*") che il clinico necessita per quel caso. Inoltre, permette una maggiore efficacia dell'approccio multidisciplinare e di telemedicina;
d) uso dinamico delle linee-guida e Percorsi Diagnostico-Terapeutici-Assistenziali ("PDTA") attraverso la realizzazione di *order-set*. Aspetto significativo per un supporto reale e costruttivo alle necessità dei medici.

La strutturazione/definizione di un *Business Glossary* comune e condiviso fra tutti gli OOSS ha importanti finalità:

a) ridurre la frammentazione della gestione del paziente, con particolare riguardo al paziente cronico dove la storia clinica è "trattata" da molti soggetti. Questo è uno degli obiettivi primari della PNT. Ciò significa rendere più omogenea la qualità clinica, a livello non solo regionale, ma nazionale, la presa in carico e il *follow-up* dei soggetti complessi (grazie all'aderenza a PDTA e linee-guida), così da garantire il paziente della migliore trattazione clinica con tutte le conseguenze derivate, tra cui solo a titolo di esempio contenere l'indice di ri-ospedalizzazione o l'accesso improprio ai pronti soccorsi. Tutto questo con una pesante ricaduta sui costi complessivi che gravano sul SSN. In pratica, supportare i clinici non solo nella decisione, ma anche nella riduzione del rischio clinico e migliorare la qualità di vita dei pazienti ("*QoL*") è la missione di base dello strumento definito *Business Glossary* e di tutte le implicazioni su tutti gli applicativi in ambito clinico-sanitario, di cui gli specifici strumenti in ambito di telemedicina;

b) grazie alla condivisione delle informazioni e delle conoscenze tra gli OOSS - medici (e infermieri) -, rendere questo processo più fluido e personalizzato al caso clinico, anche con il supporto di tecnologie avanzate di AI/ML trasparente (pensiamo, ad esempio, a come tali tecnologie potrebbero meglio clusterizzate la popolazione al fine di operare in un ambito di reale *Population Health Management*, di cui tutte le benefiche conseguenze, per esempio, nella prevenzione primaria e secondaria;
c) arrivare a modelli di miglioramento del percorso clinico, definito "*Value-Based-Healthcare*", che, grazie a procedimenti comuni e standardizzati, valutino l'intero processo clinico e l'*outcome* in maniera oggettiva e replicabile.

Alla luce di queste considerazioni, la strutturazione di una soluzione tecnologica aperta, basata su codifiche e *standard* internazionali, che permette di trasformare le "*definizioni*" delle *best-practice* in operatività quotidiana, grazie ad una profonda integrazione con i *software* clinici, basata su standard Fhir/CQL, rappresenta una innovazione sia per i medici che per i pazienti, anche nell'ottica della continuità di cura ospedale-territorio.

Inoltre, le *best-practice* definite risultano immediatamente condivisibili con altri sistemi facenti parte del piano nazionale di trasformazione digitale, creando ulteriore valore aggiunto. Un esempio in tal senso è la possibilità di governo federato delle terminologie e sistemi di codifica, in sinergia con il FSE.

Il compito principale del *Business Glossary* è la modellazione di una serie di artefatti, definiti "*computable knowledge*", che costituiscono oggetti *software* direttamente consumabili da un'applicazione *software*.
Tra i principali oggetti gestiti figurano:

- gestione delle terminologie utilizzate nello scambio di dati gestiti nei processi di telemedicina;
- concetti clinici e mappatura con le terminologie centrali e locali;
- definizione dei casi d'uso clinici relativi ai processi di telemedicina e ai casi d'uso operativi;
- definizione delle informazioni (documenti, dati strutturati, allegati, ecc.), che devono essere gestite nei processi di telemedicina.

Il *Business Glossary*, oltre che contenere i nomenclatori nazionali e cataloghi delle prestazioni da eseguire e necessari per operare, normalizzando, a livello nazionale, tali codifiche, deve contenere i piani approvati, a livello nazionale, del PDTA di monitoraggio: ossia quali parametri, con quali tipologie di *device*, la frequenza, i criteri di monitoraggio (quanto e quando), le soglie di utilizzo standard per poter attivare azioni di *escalation* clinica, i criteri e le frequenze di reporting e, se del caso, i criteri di riconoscimento economico di tali attività, specialmente in contesti interregionali e/o eseguiti tra pazienti paganti e privati.

2.4.4. Gestione Soluzioni Telemedicina

Nell'ambito dei servizi di telemedicina, un ruolo fondamentale per il processo - e particolarmente critico per quanto riguarda la sicurezza -, lo giocano le soluzioni di telemedicina, cioè tutte le componenti *software* e *hardware* che ne consentono la fruibilità: i dispositivi medici fisici di rilevazione dei parametri vitali, le componenti applicative che pilotano i suddetti dispositivi (app di configurazione, *driver*, *gateway* di acquisizione e invio dei dati), le diverse soluzioni applicative che offrono servizi di telemedicina (centrali di monitoraggio, sistemi di video chiamata, ecc.).

Il servizio di "*Gestione Soluzioni Telemedicina*" deve, pertanto, prevedere sia la fornitura di *software* specifico per l'attività di validazione, sia il supporto consulenziale necessario per facilitare la validazione ed il successivo *onboarding* delle soluzioni di telemedicina nella PNT. L'obiettivo è quello di analizzare, anche simultaneamente, le singole soluzioni, una volta arrivata la richiesta di accreditamento, e verificare, mediante protocolli di validazione, se le stesse siano *compliant* con i requisiti stabiliti, sia funzionali che tecnologici. Il servizio ha lo scopo di supportare in tutte le sue fasi il processo di validazione delle soluzioni regionali di telemedicina, degli applicativi dipartimentali delle strutture sanitarie, degli applicativi per la gestione delle cartelle dei MMG/PLS allo scopo di garantire, preliminarmente alla loro entrata in produzione e a seguito di modifiche di qualunque natura nel corso del loro ciclo di vita, che sia garantita la corretta alimentazione, attraverso il *gateway*, di EDS e dei *registry* regionali e nazionali. Le soluzioni *hardware* e *software* in grado di erogare servizi di telemedicina saranno opportunamente censite nel Catalogo Nazionale delle Soluzioni di Telemedicina (servizio della Piattaforma Nazionale di Diffusione - "PND"). A tale scopo si richiede che la PNT sia dotata

di una componente applicativa specifica che dialoghi opportunamente con la PND e con i suoi servizi di Catalogo delle Soluzioni (per ottenere la lista aggiornata delle soluzioni di telemedicina censite) e Monitoraggio dei Dati di Utilizzo (per inviare i flussi dati di utilizzo delle soluzioni di telemedicina fruibili sulla PNT).

Per la realizzazione di questo servizio deve essere, quindi, predisposto nella PNT uno specifico ambiente tecnologico e una organizzazione di processi orientata a gestire con la massima efficacia il percorso di validazione/*on boarding* mettendo a disposizione agli interessati documentazione procedurale, di specifica e strumenti di test fruibili tramite portali e servizi *web*.

Il servizio deve consentire la gestione dei processi di verifica e test delle soluzioni da accreditare e delle loro componenti (*software* di *front end* e *back end* ed *hardware*) attraverso specifici moduli per la verifica del rispetto degli standard di sicurezza ed interscambio di informazioni, il rispetto dei criteri e standard di usabilità/fruibilità, la gestione delle campagne di test nella loro interezza attraverso la disponibilità di simulatori coerenti con gli scenari e casi d'uso oggetto di test, la conformità documentale e normativa.

In termini di ambiente tecnologico si richiede l'adozione di modelli similari a quelli utilizzati nelle procedure di accreditamento dei sistemi informativi aziendali nella cooperazione applicativa con la piattaforma regionale "SISS" (Sistema Informativo Socio-Sanitario) o nei test degli *use cases* di interoperabilità delle soluzioni aderenti ai profili IHE (*Gazelle*).

L'ambiente tecnologico adottato deve essere dimensionato per garantire scalabilità e flessibilità in uno scenario di crescente presenza di soluzioni e carico computazionale.

Una specifica organizzazione deve essere dedicata all'implementazione e gestione di questo servizio al fine di assolvere ai requisiti di sviluppo e manutenzione, redazione, assistenza e *project management*. La gestione del servizio nel suo complesso tiene in considerazione i requisiti di standard di riferimento quali ISO 17025/ISO Guide 65.

Il processo di qualifica/accreditamento deve prevedere il seguente flusso di attività, puntualmente tracciato in tutte le fasi di avanzamento:

1. presentazione della domanda di qualifica della soluzione attraverso un servizio *web* di sottoscrizione delle soluzioni;

2. a fronte di domanda correttamente presentata, attivazione della procedura di qualificazione con abilitazione alle funzionalità di test e verifica coerentemente al profilo/scenario di impiego. Esecuzione dei test di conformità ed interoperabilità;
3. esito dei test con risposta ad ogni singola richiesta, con tre possibili casistiche:
    - ammissione, ove vi sia perfetta aderenza della soluzione ai requisiti, nel qual caso si avvia l'attività di *onboarding* che contempla, tra le altre, attività di verifica periodica di mantenimento della certificazione, tracciamento dell'utilizzo in soluzioni di telemedicina, interazione con Catalogo Nazionale delle Soluzioni di Telemedicina della PND;
    - richiesta di modifica, nel caso in cui la soluzione presenti taluni requisiti non in linea, ma modificabili;
    - diniego, nel caso di assenza totale di conformità.

Al fine di ottenere un elevato grado di configurabilità della soluzione utile a far fronte a potenziali scenari evolutivi futuri, il sistema deve consentire la modifica, nonché il versionamento del flusso prima descritto attraverso l'aggiunta, modifica o rimozione di *step* di attività.

Prima di iniziare formalmente un percorso di validazione/accreditamento è necessario che la specifica soluzione di telemedicina superi, un percorso di pre-validazione che può essere condotto in autonomia dal richiedente attraverso gli strumenti e la documentazione di pubblico accesso.

Solo a seguito dell'iscrizione della soluzione tra quelle certificate, si apre la possibilità di utilizzo da parte dei fruitori finali, con contestuale attivazione del monitoraggio e trasferimento delle informazioni di rilievo alla PND.

Tutte le informazioni in merito allo stato di validazione (non validato, in corso di validazione, validato) delle soluzioni, ai verbali prodotti nei relativi test e al successivo utilizzo saranno resi disponibili al richiedente e all'Amministrazione.

Il Concessionario deve attivare, congiuntamente all'Amministrazione, le opportune procedure per verificare che le soluzioni di telemedicina già certificate mantengano l'aderenza ai requisiti, o, nel caso di modifica di questi ultimi, che le varie soluzioni siano correttamente adeguate.
Per consentire la costante verifica del mantenimento dei requisiti sino al termine della concessione, dovranno essere attivate, sul nodo centrale, tante

apposite e separate istanze di validazione e test, quante sono le soluzioni validate.

2.4.5. *Policy Role Manager*

Il "*Policy Role Manager*" è il componente centralizzato della Piattaforma, deputato alla formalizzazione delle regole che definiscono l'interazione tra i servizi e micro-servizi che compongono i moduli della soluzione di telemedicina.

Il componente deve consentire:

- la profilazione di ognuno degli attori che erogano i servizi e le relative *capability*;
- la definizione di regole per l'accesso ai servizi e ai dati gestiti, sia internamente al sistema, che da componenti esterne riconducibili ai servizi regionali. La formalizzazione delle regole consentirà agli attori del sistema di interagire nel rispetto della normativa *privacy* vigente;
- la definizione di regole omogenee per tutti gli applicativi: a fronte dello stesso consenso, tutti gli attori coinvolti devono avere un'applicazione omogenea delle regole;
- l'agevolazione del processo amministrativo e del ciclo di vita della gestione delle *policy* attraverso l'utilizzo di un catalogo condiviso.

Il "*Policy Role Manager*", nel rispetto dei vincoli specifici di un'architettura strutturata su micro-servizi, deve consentire, attraverso l'utilizzo di *standard* internazionali – tra i quali, ad esempio, XACML, "*eXtensible Access Control Markup Language*" – il disaccoppiamento delle regole dalla concreta implementazione dei servizi.

L'adozione di *standard* specifici si riflette, implicitamente, sulla modellazione relativa all'architettura interna del componente, che prevede la suddivisione in più entità, o microcomponenti, in grado di consentire ad una centrale di controllo e comando di gestire esternamente le regole di accesso alle informazioni e ai dati, così come l'erogazione dei servizi fruibili dagli operatori del sistema. Di seguito, uno schema del componente "*Policy Role Manager*":

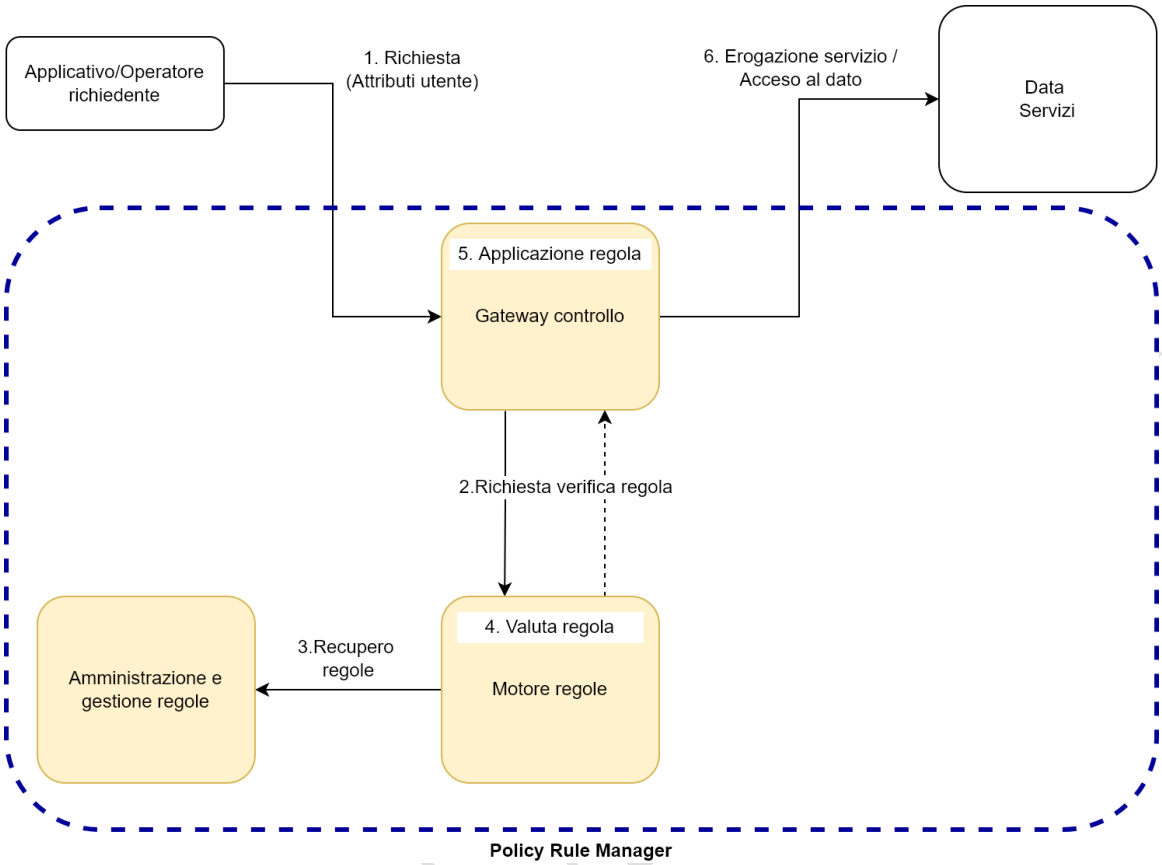


Figura 7 – Policy Role Manager

L'adozione di uno *standard* nella definizione di regole può consentire la portabilità delle configurazioni anche in contesti dove l'operatività tra servizi abilitanti e servizi minimi sia distribuita su base centralizzata, oppure ibrida.

Il componente deve garantire la possibilità di modellare scenari all'interno dei quali devono poter essere definiti servizi, dati ed attori che permettono, attraverso i rispettivi attributi, di verificare la regola specificata per l'accesso ad un'informazione.

Il componente deve basare le regole relative alla modalità di accesso ai dati sul paradigma ABAC – "*attribute-based access control system*". Questo modello architetturale consente di gestire l'accesso all'informazione e l'erogazione di un servizio in funzione di un insieme di attributi recuperati dall'utente e dal contesto. Per realizzare questo modello è necessario:

- il censimento di un catalogo di risorse e di utenti;
- la dichiarazione degli attributi propri di ogni entità convolta nei processi (utenti e servizi). A corollario di queste, la definizione sul componente *Business Glossary* delle codifiche da utilizzare;

- la cooperazione funzionale con il componente IAM. Tale elemento, previsto nell'architettura, consente di recuperare gli attributi relativi agli utenti, che sono gestiti attraverso l'utilizzo di *token* SAML2/Oauth 2.0 all'interno di una modalità di autenticazione federata;
- la sinergia con i *Servizi Raccolta Dati*, garantendo *by design* e *by default* il rispetto della normativa GDPR;
- l'integrazione con il *repository* dei consensi.

2.4.6. Motore di *Workflow*

In un contesto che intende la soluzione di telemedicina come mirata alla semplificazione dell'attività clinica, il Motore di *Workflow* non deve essere soltanto inteso come uno strumento tecnologico, bensì come un elemento fortemente interconnesso e di ausilio alle attività cliniche.

Il componente Motore di *Workflow* rappresenta un elemento fondante dell'architettura della PNT, contribuendo all'organizzazione degli assetti e degli scenari clinici e consentendo, quindi, di garantire il corretto accoppiamento funzionale tra le componenti distribuite su base regionale/aziendale e quelle presenti sull'infrastruttura centrale. Deve, inoltre, favorire la corretta cooperazione tra i servizi abilitanti e i servizi regionali.

Il componente Motore di *Workflow* deve garantire le seguenti funzionalità:

- integrazione con sorgenti di informazioni e applicazioni esterne: API REST, *web-app hook*, *database* e *code* JMS;
- creazione di connettori specifici, che consentano una facile integrazione con un *server* FHIR;
- possibilità di avanzamento ed interazione attraverso: *data-driven task*, API Rest e *human task*;
- orchestrazione delle interazioni sia all'interno di una singola applicazione, che tra tutte le applicazioni afferenti alla Piattaforma.

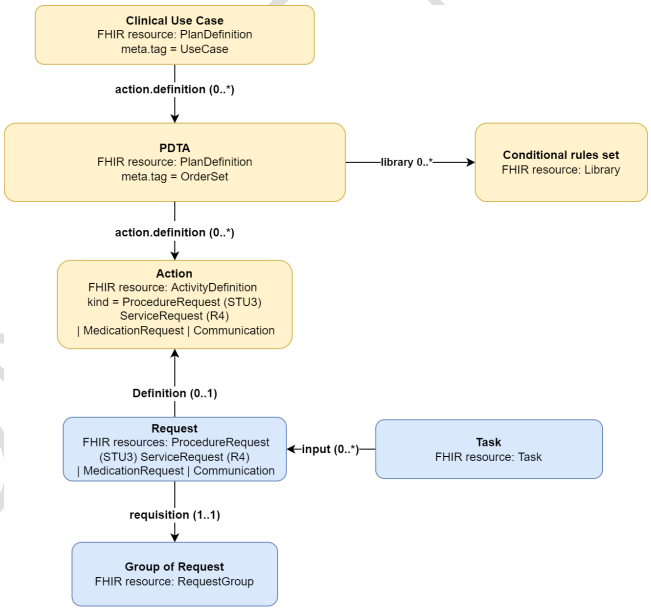
Il Motore di *Workflow* deve prevedere interfacce utente per la configurazione, che ne incentivino l'utilizzo. Tale obiettivo deve essere raggiunto sia attraverso l'adozione di interfacce intuitive e fruibili che tramite strumenti e metodologie *standard*.

Il Motore di *Workflow* deve lavorare strettamente con il componente di *Business Glossary* andando a definire i casi d'uso clinici.

Il caso d'uso clinico, definito "*Clinical Use Case*" (o "Cuc") circoscrive, essenzialmente, un processo, inteso come elenco di azioni, o gruppi di azioni che devono essere eseguite su un paziente che si trova ad essere parte di un determinato contesto clinico.

Esempio di *Clinical Use Case* è il concetto di PDTA, inteso come metodologia mirata alla condivisione dei processi decisionali e dell'organizzazione dell'assistenza per un gruppo specifico di pazienti per un periodo di tempo ben definito, che dovrà essere rappresentato nel *Business Glossary* mediate una struttura FHIR di tipo *PlanDefinition*/*ActivityDefinition*.

Per "azioni" - definite "*Action*" nello schema che segue -, si intende azioni di tipo clinico-terapeutico, che possono, però, essere dettate anche da informazioni legate a fattori economici: nel caso del tele-monitoraggio, ad esempio, il numero di registrazioni di uno specifico parametro viene definito non solo in base alla valenza clinica, ma anche alla modalità di riconoscimento del rimborso economico.



Lo schema illustra la relazione tra le entità definite dal *Business Glossary* nel contesto della gestione dei PDTA. Il *Business Glossary* declina il PDTA definendo una serie di azioni cliniche ed assistenziali contestualizzati agli specifici contesti operativi - *stage* - definiti *Cuc*, che devono essere eseguite

su un paziente aderente allo specifico caso clinico. A seconda del quadro clinico del paziente, del contesto operativo e della fase della patologia, ed anche in contesti di una o più co-morbilità, vengono declinate le azioni da eseguire sul paziente, tra cui, ad esempio, la tipologia di telemonitoraggio, la tipologia di *device*, la frequenza delle rilevazioni, le soglie di intervento, le tipologie e frequenze di *reporting*, i criteri di *escalation*.

Il piano può, o meno, prevedere una condizionalità delle azioni definita da regole condizionali contenute in una struttura FHIR separata, collegata al piano di trattamento, chiamata "*Library*". Le strutture che mappano le azioni costituiscono, di fatto, un *template* per le azioni effettivamente previste nel processo clinico - definito "*Request*" nello schema che precede -, e da queste istanze vengono referenziate.

Infine, come parte del processo, ogni *Request* può, eventualmente, far capo a un raggruppamento di attività, "*Group of Request*", ed essere tracciata da una struttura di tipo *Task*, con l'obbiettivo di gestirne lo stato all'interno del processo.

Tutte queste definizioni e regole devono essere fruite secondo API basate su standard FHIR e, quindi, essere usate in tutti i contesti clinici ed assistenziali, tra cui tutti i contesti eseguibili in telemedicina.

Le azioni del processo vengono condizionate da una serie di regole cliniche che rappresentano i criteri stabiliti dal PDTA, i quali, se rispettati, fanno avanzare il paziente alla fase successiva dell'indagine clinica.

2.5. Architettura Fisica

Il presente paragrafo descrive le caratteristiche previste per architettura fisica che eroga la PNT, inclusa delle componenti nazionali, di interoperabilità e sicurezza.

L'architettura è disegnata in modo da essere scalabile ed adattabile; quindi, pronta a modellarsi alle richieste ed alle evoluzioni delle altre progettazioni nazionali, a cominciare dal FSE Nazionale e FSE 2.0.

2.5.1. *Cloud Readiness*

L'intera soluzione individuata per la Piattaforma deve essere progettata e costruita nativamente secondo i principi del *cloud*, basandosi su un'etica che

contempli elevati livelli di disponibilità e capacità di scalabilità elastica, fornendo, di fatto, la soluzione nelle modalità PaaS o SaaS.
L'architettura deve essere basata sul paradigma dei micro-servizi e prevedere livelli aggiuntivi di sviluppo per integrare le tecnologie di containerizzazione, orchestrazione, interfacce di programmazione delle applicazioni (API), *routing* e sicurezza.

2.5.2. Containerizzazione

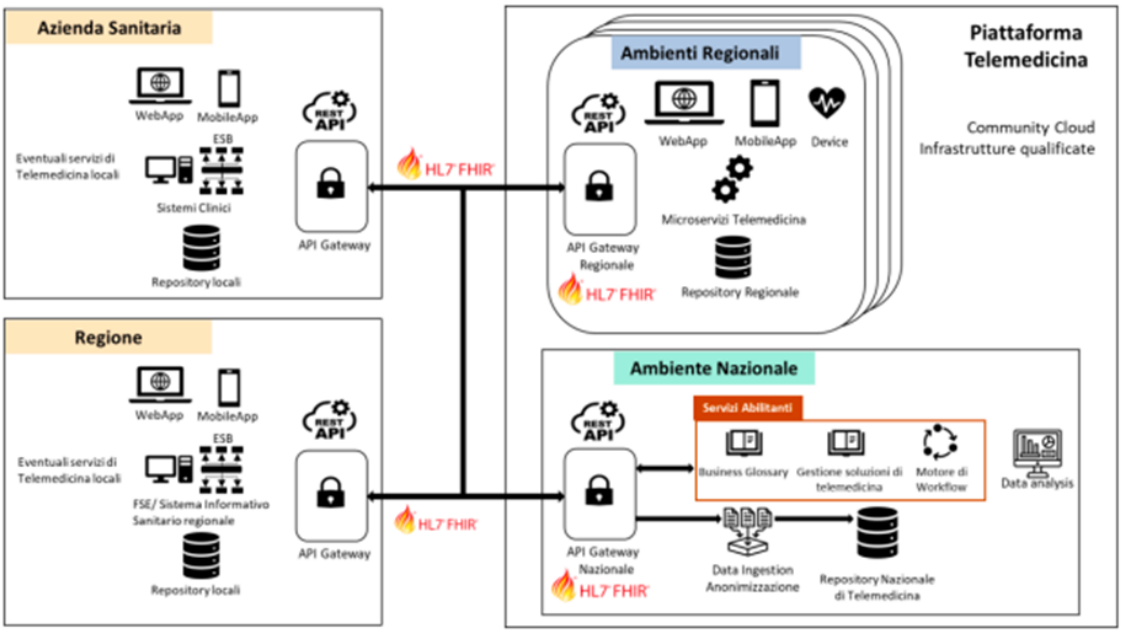
L'ecosistema architetturale della soluzione individuata per la Piattaforma, in termini tecnologici relativi alla gestione delle istanze applicative, deve prevedere l'utilizzo dei *container*, al fine di isolare il *software*, consentendone l'esecuzione, in modo indipendente, su diversi sistemi operativi, *hardware*, reti, sistemi di *storage* e criteri di sicurezza.
Al fine di evitare, anche in questo contesto, legami con *vendor* specifici, la tecnologia adottata per la containerizzazione deve essere conforme alla *Open Container Initiative*, iniziativa che ha come obiettivo la creazione di *standard* di formato e di esecuzione.

2.5.3. Architettura Fisica

Infrastruttura
La PNT prevede una architettura tecnica a copertura delle seguenti macro-componenti:

- istanza (Nodo) Centrale/Nazionale: dedicato ai servizi abilitanti a livello centrale
- istanze Regionali: istanziati sempre a livello centrale, con un livello di isolamento elevato, erogano eventuali servizi dedicati ai moduli dei servizi abilitanti alla integrazione.

-



La Piattaforma deve essere interamente erogata su *Public Cloud*, in architettura *multi availability zone* e istanziata su due *region* distinte per l'erogazione e di *disaster recovery*.
L'ambiente relativo alla Piattaforma è modellato sulla base di:

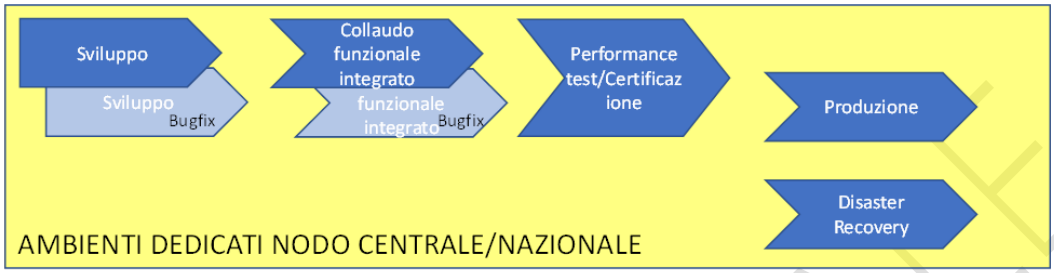
- *building blocks* erogati su *cloud* pubblico per la realizzazione di tutti i requisiti funzionali;
- Piattaforma infrastrutturale di erogazione dei micro-servizi basata sulla *suite* RedHat Openshift o similari, assettizzata nella soluzione definita *Hybrid Cloud* GEN3 (descritta nel seguito del PTAS). Questa Piattaforma deve essere gestita centralmente secondo principi di *continuous e seamless update*, *zero downtime deployment* e inclusivo di tutte le *capability* di gestione (SDN, *Backup*, *Monitoring*, *Security*, ecc.).

La Piattaforma ospita i dati integralmente cifrati tramite una architettura basata su HSM (*Hybrid Security Module*), che mantengono la chiave di decrittazione dei dati su *datacenter* distinti da quelli di erogazione dei servizi, ridondati su *region* multiple e collocati sul territorio nazionale italiano.

2.5.4. Ambienti PNT

Il Nodo nazionale deve disporre di ambienti dedicati per tutto il ciclo di vita.

Nodo Nazionale:



Gli ambienti di sviluppo e collaudo devono essere in grado di gestire sia l'evoluzione delle componenti che attività di manutenzione correttiva (*bug fixing*).
Gli ambienti di *Disaster Recovery* (o "DR") e Certificazione/*Performance test* devono avere un dimensionamento pari all'ambiente di produzione, ma attivati su richiesta, al fine di ottimizzare la produzione e, quindi, il relativo costo.
In particolare, l'ambiente di *Disaster Recovery* deve prevedere l'accensione continuativa con risorse minimali, e delle sole componenti per le quali non sia possibile la creazione via IaC in tempi estremamente limitati e compatibili con l'RTO previsto. Devono, invece, essere attive con continuità tutte le componenti di replica dati (in modo esplicito o incluso nel livello di *business critical* identificato nella creazione dei PaaS).

L'approccio per la definizione degli ambienti di produzione, DR secondo il paradigma di *Infrastructure as code* permette di rendere disponibile un ambiente precedentemente modellato in tempi estremamente limitati (ore), inoltre il *sourcing* su *public cloud*, abilita la possibilità di scalare oltre il numero di filiere previste in caso di *change* che richiedano un aumento delle performance.

2.5.5. Componente hybrid cloud

Allo scopo di garantire l'*encryption* dei dati (*at rest* per *short* e *long term retention* ed *in transit*) e la capacità di garantire la indecifrabilità, la soluzione di cifratura deve essere basata su istanze multiple di HSM ridondati e distribuiti su *Data Center* ("DC") esterni al *cloud provider*.
I DC coinvolti devono essere collocati in architettura Campus e su due regioni distinte, entrambe collocate su territorio italiano.

In questi DC deve essere memorizzata la chiave di cifratura/decifratura dei dati, che risulta, quindi, del tutto inutilizzabile sia in caso di furto dal *cloud provider*, che in caso di spostamento su *region* del *cloud provider* non autorizzate alla persistenza di dati di cittadini italiani.
La soluzione implementata deve essere interamente basata su soluzione *Zero Trust Architecture*.

2.5.6. Sicurezza Infrastrutturale

La Piattaforma deve implementare le soluzioni atte a garantire i servizi di accesso e sicurezza infrastrutturale:

- *Firewalling* e DMZ;
- VPN *concentrator*;
- Infrastruttura Proxy;
- Strumenti di DDOS *prevention* e IDS (*Intrusion Detection Systems*);
- Strumenti di URL/*Web filtering*;
- Infrastruttura di *Backup*;
- *Log auditing*;
- *Log collection*;
- SIEM (*Security Information Event Manager*).

Allo scopo di limitare la possibilità di *injection* di *malware* e virus, inoltre, la Piattaforma deve essere resa accessibile agli amministratori unicamente tramite un *layer* di *Virtual Desktop Infrastructure*.
Tutti gli accessi ai sistemi devono essere protetti e gestiti tramite soluzioni di *Privileged Access Management*.
Tutti gli accessi, a VPN, servizi e applicazioni, devono essere protetti da MFA.
Infine, devono essere resi disponibili strumenti di *Data Loss Prevention*.

2.5.7. Connettività

- DC *on prem vs* DC *on prem*: i DC *on prem* dislocati sulle *region* devono essere connessi da *link* ad alta velocità multi-ridondati e dimensionati per garantire latenze nelle repliche dati sincrone (CAMPUS) e asincrone (DR) che abilitino RPO = 0 e latenze <10ms (DR);
- DC *on prem vs* Internet: i DC *on prem* devono essere connessi al *backbone* internet, tramite *link* dedicati multi-ridondati e forniti da *carrier* nazionali;
- DC *on prem vs Cloud provider*: la connessione deve essere basata su connessioni private (es: *ExpressRoute*).

2.5.8. Asset Hybrid Cloud

La soluzione *Hybrid Cloud* deve essere realizzata tramite un *asset container platform enterprise ready*, basata su un *core open source*, e ingegnerizzata per realizzare compiutamente le strategie di *cloud* ibrido, *multicloud, edge*.
La Piattaforma deve implementare caratteristiche di automazione e controllo, per esempio quelle offerte da *kubernetes*, arricchita con estensioni.
La Piattaforma deve prevedere la possibilità di rendere disponibile un *cluster*, qualora necessario, entro 48 ore, su *baremetal* o *cloud*, con un processo codificato e riproducibile.
La soluzione deve implementare una Piattaforma sicura, *multi-tenant* e *multi-cluster* con un isolamento completo dello *stack* e una segregazione dei ruoli per una gestione indipendente dei *tenant* di applicazioni.
La Piattaforma deve includere una *consolle* tramite la quale si accede ad un catalogo di soluzioni certificate da *partner*, e soluzioni *custom*, liberamente documentabili e distribuibili.
Gli strumenti centralizzati di gestione riducono i costi e gli impegni di esercizio, riducendo i *drift* di configurazione, gli errori di implementazione e implementando i *single pane of glass* per il *DevSecOps* su infrastrutture e applicazioni.

DC HYBRID SERVICES

La Piattaforma realizza servizi di *Data center* ibridizzati, che abilitano modalità di *delivery*, aggiornamento e gestione indipendenti dall'ambiente *target* che realizza l'*hosting*.
Alcuni di questi servizi:

- DNS: sistema integrato per la gestione di domini privati, pubblici e di servizi avanzati;
- URL Filtering: sistema per la protezione delle connessioni verso Internet;
- WAF/CDN: sistema per la protezione e la scalabilità dei servizi esposti su rete pubblica;
- *Log Collectors*: sistema integrato per il collezionamento *long-term* di *log* operativi e di *audit;*
- *Load Balancer*: sistemi per il bilanciamento del carico;
- AD/LDAP: autenticazione integrata AD/AAD e federazione AAD per i *service account;*
- *Storage*: integrazione con i sistemi locali di *storage* e presentazione di *storage class* omogenee di tipo a blocchi, *file* e *object;*
- *Management systems*: integrazione nativa con RHACM e RHACS per la centralizzazione delle *devsecops;*
- *Globalsign*: per la generazione e verifica di validità dei certificati SSL.

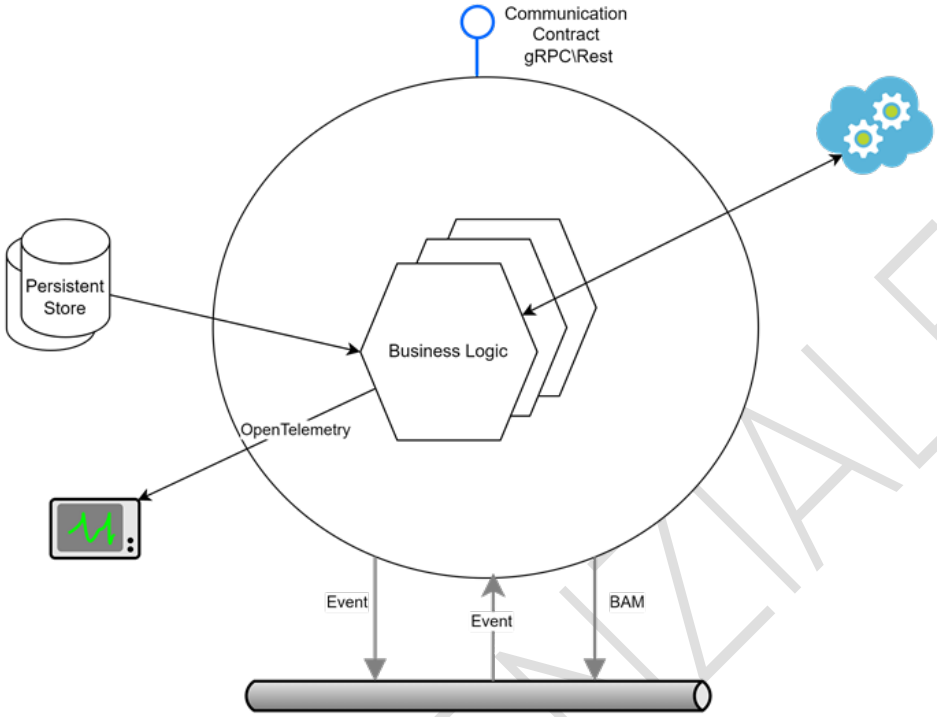
ALM

L'integrazione con i servizi di ALM consente di gestire il *deployment* del *cluster* stesso, nonché realizzare la CI/CD (Integrazione continua/*Deployment* continuo) per i servizi che il *cluster* ospiterà.

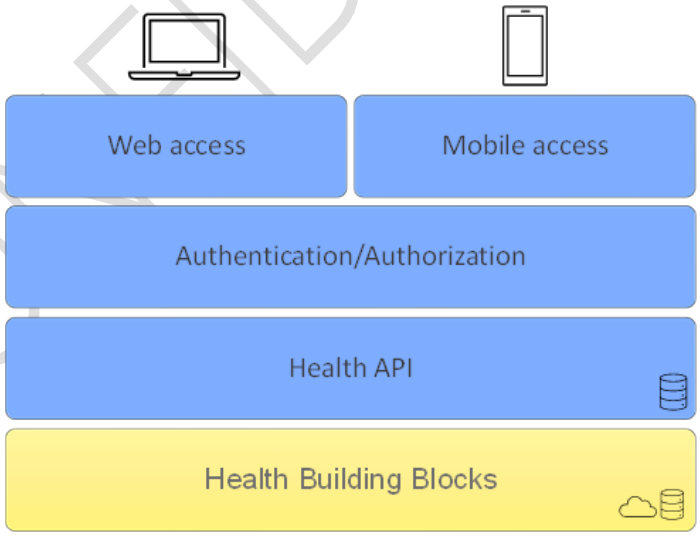
2.5.9. PNT – *Building Blocks Approach*

Il *building block* è un'entità logica che deve avere le seguenti caratteristiche:

- deve fornire una singola funzionalità autoconsistente. Per "*autoconsistente*" si intende che deve fornire tutte gli strumenti necessari all'erogazione della funzionalità;
- può utilizzare servizi *Cloud* a valore aggiunto. Deve essere, per quanto possibile, *Cloud Independent*;
- non deve dipendere direttamente da altri *building block* o sistemi esterni;
- può essere formato da uno o più micro-servizi;
- può utilizzare uno o più *storage* di archiviazione NON condivisi con altri *building block*;
- espone contratti di comunicazione ben definiti secondo lo standard "*Open* Api";
- le API non sono mai esposte pubblicamente, non possono essere accedute direttamente dall'applicazione di *front end* e, quindi, devono essere invocate dal *layer* contenente la logica di *business* della specifica applicazione;
- offre una documentazione esaustiva;
- deve essere osservabile.



Le *capabilities* infrastrutturali saranno, garantite da un *layer* dedicato di servizi per autenticazione, autorizzazione, cifratura dei dati "*at rest*".



La soluzione definita tramite *building blocks* per le funzionalità erogate su nodo nazionale si deve, quindi integrare con il *layer* infrastrutturale per le

componenti di sicurezza, e con gli strumenti di *log collection*, *audit* e APM per il monitoraggio.

2.5.10. *Privacy* e *Compliance* GDPR (Infrastrutturale)

Come riportato nello specifico capitolo 4 del PTAS, il D.Lgs. 196/2003 e ss.mm.ii. (Codice in materia di protezione dei dati personali, di seguito il "Codice Privacy") e il GDPR, nonché i Provvedimenti emanati dall'Autorità Garante per la Protezione dei dati personali, si prefiggono di garantire che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

Il Codice Privacy stabilisce, in particolare:

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

Nell'ambito delle attività, il Concessionario deve garantire la piena aderenza ai principi ed alle normative citati, secondo un processo coerente con quanto previsto dal capitolo 4 del PTAS e con servizi che sono descritti nel Gestionale.

3. Il *Layer* Interoperabilità

Lo strato o *Layer* Interoperabilità ricopre un ruolo rilevante all'interno della soluzione PNT. Tale elemento deve essere in grado di facilitare la cooperazione tra i servizi centrali (quali SPID/CIE, ANA, PagoPA, etc.), i servizi abilitanti, messi a disposizione dalla PNT, e le componenti aziendali. Quest'ultima integrazione riveste un ruolo fortemente strategico ed è per questo che il *Layer* Interoperabilità deve garantire flessibilità, scalabilità e adattabilità ai differenti contesti locali, in considerazione della eterogeneità delle soluzioni esistenti e della loro naturale evoluzione.

L'architettura della Piattaforma prevede l'adozione dello *standard* HL7/FHIR come modello di interoperabilità sintattico-semantica. Dal punto di vista applicativo, le interazioni avvengono utilizzando servizi, API REST, protetti attraverso l'uso del protocollo OAuth 2.0. Sono previsti nodi API *Gateway* HL7/FHIR sia sull'ambiente centrale che sugli ambienti regionali PNT, in modo da garantire una comunicazione "*aperta*" e basata nativamente sullo *standard*.
L'API *Gateway* consente, infatti, l'integrazione tra la PNT e gli altri componenti dell'ecosistema sanitario regionale. Lo scopo è quello di ridurre l'impatto sulle installazioni e ottimizzare la sostenibilità dell'operazione. Devono, pertanto, essere previsti più modelli di utilizzo, in grado di garantire che siano soddisfatti i livelli eterogenei di integrazione con gli API Gateway aziendali e regionali. Di seguito, un elenco delle possibili modalità:

- ***Integrazione SDK***. In questo scenario, è prevista la fornitura di un componente SDK con lo scopo di favorire e abilitare l'integrazione del *gateway* HL7/FHIR, installato localmente, con gli applicativi in uso presso l'AS e/o la Regione. L'adozione di questo componente consente di ridurre l'impatto sugli applicativi locali e, al tempo stesso, accelerare l'integrazione con i servizi esposti dai moduli centrali della PNT;
- ***Integrazione tramite API***. Integrare il *gateway* HL7/FHIR attraverso l'uso delle API costituisce, dal punto di vista architetturale, la soluzione da privilegiare, in quanto assicura un approccio interoperabile "*by design*", garantendo una maggiore capacità di collaborazione tra le componenti locali di telemedicina e i servizi centrali e regionali;
- ***Utilizzo moduli della Piattaforma***. Questa modalità trova la sua applicazione in quei contesti locali in cui le applicazioni non riescono ad utilizzare il componente SDK e le API messe a disposizione dalla PNT per l'integrazione con l'API *Gateway* locale. In questo scenario, per assicurare un approccio scalabile e ridurre l'impatto sugli applicativi locali, la PNT deve rendere disponibile, sulla componente centrale, un

set di servizi e di interfacce che consentano una chiamata in contesto da parte degli applicativi locali.

Gli aspetti sopracitati, relativi all'interoperabilità, sono ulteriormente enfatizzati alla luce della integrazione e della cooperazione della PNT con i sistemi di gestione documentale esistenti, quali gli FSE regionali. A livello di infrastruttura nazionale, è prevista, infatti, l'introduzione di un EDS, verso il quale è atteso l'invio di dati da parte della PNT, delle strutture sanitarie e degli FSE regionali.

Il *Layer* Interoperabilità, in ogni caso, deve essere rispondente alle evoluzioni delle altre iniziative nazionali; quindi, il Concessionario nelle fasi di progettazione e sviluppo, deve tenerne conto.
Peraltro, l'aderenza alle iniziative nazionali deve essere garantita durante tutta la Concessione, ed in particolare nella c.d. fase di consolidamento, così come previsto nel Gestionale, grazie anche al riuso di componenti da e per la PNT.

Anche questa integrazione richiede uno scambio dei dati, che deve essere supportato in modalità bidirezionale.
In considerazione delle caratteriste della nuova infrastruttura FSE 2.0, con la quale la PNT deve armonizzarsi, deve essere garantito il rispetto delle seguenti linee guida:

- protocolli di comunicazione API REST basati sullo *standard* HL7/FHIR e protetti attraverso l'utilizzo del *framework* di autenticazione OAuth 2.0;
- scalabilità e facilità di orchestrazione nel rispetto delle progettualità esistenti e delle corrispondenti evoluzioni.

3.1. Interoperabilità con i servizi centrali

Tutti i servizi esposti dalla PNT devono, in ottemperanza alle linee guida definite nel Piano AGID, essere integrati con i servizi messi a disposizione dalla PDND della PA.

L'adozione di questo modello ha lo scopo di semplificare la cooperazione tra le PA utenti e, al tempo stesso, migliorare l'esperienza utente per il cittadino, che non deve utilizzare credenziali diverse per l'accesso ai servizi. Il paradigma definito dalla PDND consente di rispettare le indicazioni dell'Unione europea, attuando il principio "*once only*" e, al tempo stesso, il rispetto del concetto di minimizzazione previsto dal GDPR.

Il modello organizzativo previsto dalla PDND consente al sistema di telemedicina di utilizzare le API messe a disposizione da servizi esistenti. Di seguito, un dettaglio dei servizi:

- Sistema SPID/CIE

  Entrambe le componenti consentono di effettuare le attività di autenticazione ed accesso ai servizi. Per gli OOSS, deve essere prevista l'integrazione per il recupero del profilo e degli attributi utente, necessari all'erogazione del servizio, con i servizi del componente IAM.

- FSE Nazionale

  La PNT deve essere integrata con i servizi del FSE Nazionale in una modalità bidirezionale, che prevede il recupero delle informazioni e dei documenti clinici relativi al paziente necessari al processo di cura e l'alimentazione dello stesso con gli esiti e le risultanze prodotti a valle del percorso di cura mediante l'uso degli altri servizi della PNT.

- ANA

  La Piattaforma deve prevedere l'integrazione con i servizi forniti da ANA, sia per l'identificazione e il recupero dei tratti anagrafici degli assistiti, che per l'acquisizione dei dati relativi all'assistenza sanitaria, ovvero le informazioni sugli MMG per i dati anagrafici degli assistiti e l'identificazione dei MMG/PLS ad essi associati; ANA è utilizzata direttamente dal GW, dal *Data Repository* Centrale e dal *Registry* Nazionale.

- PagoPA

  La PNT deve essere in grado di interfacciarsi con i servizi di pagamento, consentendone la fruizione per l'erogazione delle prestazioni agli assisiti.

- Sistema TS

  L'integrazione con il Sistema TS consentirà alla PNT di recuperare le informazioni relative alla gestione amministrativa, che si rendono necessarie per la corretta esecuzione di un percorso terapeutico.
  Nello specifico, l'integrazione con il Sistema TS consentirà sia il recupero delle esenzioni e delle prescrizioni elettroniche, che la verifica della congruità dei piani terapeutici.

Al tempo stesso, la PDND consentirà di rendere fruibili le funzionalità e i servizi erogati dalla Piattaforma attraverso la pubblicazione di API conformi allo *standard* e ai *pattern* definiti dal *Layer* Interoperabilità.

3.2. Interoperabilità con i dispositivi medici

L'interoperabilità con i dispositivi medici deve essere realizzata in modo da garantire il supporto:

- dello *standard* ISO/IEEE 11073 SDC;
- dei profili IHE del dominio PCD (già *standard* Continua);
- dello scambio dati mediante HL7/FHIR, come definito dal progetto GEMINI promosso da HL7 International e IHE.

4. Cybersicurezza

Nel presente capitolo del PTAS, si riportano le attività che devono essere previste al fine di **assicurare riservatezza, integrità e disponibilità** dei dati e che, quindi, devono, in ogni caso, essere adottate dalla Piattaforma, considerando che tutte le operazioni sui **dati personali e sanitari** del cittadino necessarie per l'erogazione di servizi di telemedicina rientrano tra i trattamenti di dati **c.d. "*particolari*",** effettuati mediante strumenti elettronici, che sono regolati dalle disposizioni del GDPR.

In particolare, deve essere assicurata la conformità ai requisiti minimi descritti nelle circolari AGID n.ri 2 e 3 del 2018 in materia di requisiti per la qualificazione dei *Cloud Service Provider* per la PA, e garantito, per tutti i servizi applicativi e loro componenti, il rispetto delle "*Misure minime di sicurezza ICT per le Pubbliche Amministrazioni*", di cui alla Circolare AGID n. 2/2017.

La crittografia della comunicazione tra *client* e *server* deve essere basata sul protocollo TLS 1.3 e allineata con la Determinazione AGID n.471 del 5 novembre 2020 – "*Adozione delle Raccomandazioni AgID in merito allo standard Transport Layer Security*".

La PNT deve assicurare la conformità alla norma UNI EN ISO 27001: 2013 e alle linee guida ISO/IEC 27017:2015 (Linee guida per la sicurezza dei servizi *Cloud*) e ISO/IEC 27018:2019 (Linee guida per la protezione dei dati personali nell'ambito di servizi *Cloud*), su canali cifrati e su *database* sicuro e protetto da crittografia.

La direttiva europea NIS2, al momento solo in forma di proposta ma di prossima introduzione, impone l'adozione di misure di gestione del rischio di cybersicurezza anche per il settore sanitario quale "*entità essenziale*". Pertanto, la PNT deve conformarsi alla direttiva NIS2 e rispettare gli aspetti cardine relativi all'approccio basato sull'analisi del rischio, la verifica della *Supply Chain* ed i nuovi requisiti per la risposta agli incidenti.
La Piattaforma deve essere dotata di una componente applicativa per il tracciamento delle azioni svolte, sia in termini di utilizzo della Piattaforma, che rispetto ad eventuali trasformazioni operate sui dati. Tale requisito deve essere garantito anche alla componente documentale: infatti, il *Repository* che dialoga con i servizi di erogazione delle prestazioni di Telemedicina deve

consentire la storicizzazione dei documenti prodotti, al fine di garantirne una conservazione coerente rispetto alle finalità di utilizzo.

Infine, il sistema deve rendere disponibile una soluzione di identificazione e tracciamento delle anomalie, eventualmente fraudolente, nei dati gestiti, anche facente ricorso a tecniche di AI.

4.1. Security By Design

Lo scopo del presente paragrafo è definire le azioni che devono essere svolte in tema di *IT Security* e di *Data Protection* dalle varie parti interessate (*stakeholder*), ciascuno per la propria competenza, nei processi operativi di realizzazione dei prodotti/servizi IT al fine di integrare la sicurezza *by default* e *by design*.
Obiettivi delle suddette azioni sono:

a) **prevenire gli impatti economici, legali e di immagine** che possono essere causati da incidenti di *cybersecurity* e/o *data breach*;
b) **valutare correttamente i costi** per la realizzazione di un prodotto/servizio sicuro, ossia, conforme ai principi di *Security* e *Privacy by design* e *by default*;
c) **evitare** il **costo elevato** ed il **consistente impatto operativo** degli interventi sulla sicurezza eseguiti "*a posteriori*" nel ciclo di vita del prodotto/servizio;
d) **ottenere la *compliance*** alla normativa europea e nazionale in termini protezione dei dati personali, ossia il GDPR, ed alle disposizioni relative alla sicurezza previste dalle normative cogenti applicabili (ad esempio Codice dell'Amministrazione Digitale per la PA, disposizioni e circolari della Banca d'Italia in ambito Finance, NIS per le infrastrutture critiche, etc.);
e) **rispettare gli *standard* tecnici previsti** dal sistema di gestione integrato certificato (ISO 27001, ISO27017, ISO27018, etc.);
f) **concorrere** al **vantaggio competitivo** derivante dal miglioramento del ciclo produttivo e della qualità del prodotto/servizio.

4.1.1. Classificazione del dato

La *security&privacy by design* necessita di un primo passaggio di classificazione, ai fini della sicurezza e *privacy*:

- dei servizi e degli *asset* interessati,
- degli ambienti di elaborazione.

La classificazione dei servizi e degli *asset* si applica a **sistemi, servizi, prodotti, applicazioni e/o dispositivi** in funzione dei dati che, attraverso di essi, vengono trattati (classificazione *data driven*). Si riportano, di seguito, i criteri per la classificazione:

	Classificazione dato			
	Critico	Alto	Medio	Basso
Dati particolari (GDPR) o dati critici per il *business*	x			
Dati personali		x		
Dati generici / pubblici			x	
Dati test				x

Gli ambienti nei quali i dati sono trattati sono, invece, classificati come segue:

	Classificazione progetto			
	Critico	Alto	Medio	Basso
(ambiente di) Produzione con dati particolari (sia esposto su internet che non) o dati critici per il *business*	x			
(ambiente di) Produzione esposto su internet con dati personali		x		
(ambiente di) Produzione esposto su internet *no privacy*			x	
(ambiente di) Produzione non esposto su internet con dati personali			x	
(ambiente di) Produzione non esposto su internet *no privacy*			x	
(ambiente di) Non Produzione (es. Sviluppo) esposto su internet			x	
(ambiente di) Non Produzione (es. Sviluppo) non esposto su internet				x

Per gli ambienti di non produzione, nel rispetto della normativa sulla protezione dei dati personali, in considerazione dell'elevato rischio sul *business* e delle raccomandazioni ISO27001 e ISO27002, non è consentito l'utilizzo di dati reali.

Rimane inteso che qualsiasi altra situazione deve essere, opportunamente, valutata ed inserita nella classificazione di cui sopra.

4.1.2. *Baseline* di sicurezza

Successivamente alle operazioni di cui *sub* 4.1.1., in funzione della classificazione del **sistema, servizio, prodotto, applicazione e/o dispositivo,** per ciascuna macro-fase del ciclo di vita del prodotto/servizio e tipologia di architettura (*On Premise*/*Cloud* IaaS, PaaS, Saas, Faas), deve essere individuata la ***baseline*** **delle misure di sicurezza**, che devono essere applicate, come, schematicamente, descritto di seguito.

Le misure di sicurezza indicate sono delle seguenti tipologie:

- misure **preliminari:** devono essere previste nella fase di **definizione della architettura**;
- misure **preventive:** devono essere previste nella fase di **definizione e** *delivery*:
  - della **infrastruttura** *On Premise* o IaaS;
  - del ***middleware*/applicazione** *On Premise*, Paas o FaaS;
- misure di **verifica** e **validazione** devono essere previste nella fase di **sviluppo o acquisizione** di una applicazione;
- misure che devono essere previste nella fase di **erogazione/esercizio**.

4.1.3. GDPR Compliance e Privacy Assessment

Il Codice Privacy e il GDPR, nonché i Provvedimenti emanati dall'Autorità Garante per la Protezione dei dati personali, si prefiggono di garantire che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

Il Codice Privacy stabilisce, in particolare:

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

Nell'ambito delle attività sulla PNT, il Ministero della Salute quale Titolare nomina Agenas Responsabile del Trattamento, mentre il Concessionario sarà nominato "sub-*Responsabile del trattamento dei dati personali*" ("**RTDP**"), ai sensi del GDPR. È compito del RTDP procedere a designare e formare opportunamente come "*Incaricati*" i soggetti (persone fisiche) preposti al trattamento dei dati e a designare come "*Amministratori di Sistema*" i soggetti preposti a tale funzione, indipendentemente dalla sede da cui operano.

Il Codice Privacy definisce un insieme di misure (cfr. artt. 33, 34, 35) che devono essere applicate, con lo scopo di assicurare un livello minimo di protezione dei dati personali. Oltre all'applicazione delle misure di sicurezza, il trattamento dei dati personali, da parte del Concessionario, incluso qualsiasi suo *sub*-fornitore, deve sempre ispirarsi al rispetto dei principi generali del

Codice Privacy e del GDPR e, quindi, avvenire in modo lecito e secondo correttezza, valutando la pertinenza, la completezza e la non eccedenza dei dati rispetto alle finalità dei trattamenti in funzione delle attività assegnate.

Inoltre, come previsto dal GDPR, deve essere adottato un approccio basato sulla *Security* e *Privacy by Design* e *by Default*, che prevede l'adozione di adeguate misure di sicurezza a tutela di tutto il ciclo di vita del trattamento dei dati personali.

Si devono applicare con continuità i principi esposti e ad attivare, nell'ambito della Concessione, un processo di ***privacy assessment***, finalizzato ad identificare eventuali *gap* rispetto a quanto richiesto dal GDPR in termini di processo.

4.1.4. *Security Assessment*

Basandosi sui risultati ottenuti dalla classificazione dei dati e definite le *baseline* per ogni elemento, deve essere definita una pianificazione delle analisi di sicurezza, suddividendo queste ultime per gli specifici livelli, nel dettaglio:

- Livello codice sorgente
  - *Code Review*
  - *DevSecOps*
- Livello infrastruttura
  - *Vulnerability Assessment*
  - *Penetration Test*
- Livello applicativo
  - *Vulnerability Assessment*
  - *Penetration Test.*

Le analisi di Sicurezza - denominate ***Vulnerability Assessment*** - devono essere eseguite utilizzando strumenti automatici in grado di rilevare le vulnerabilità, in modo da garantire l'esercizio dei sistemi, riducendo le probabilità di disservizio e la numerosità dei falsi positivi. Infine, deve essere adottata una soluzione in grado di mostrare i risultati in tempo reale, da remoto, tramite interfaccia *web* centralizzata, contenente grafici e contenuti personalizzabili e supporto API.

Per garantire una maggiore capacità di rilevazione, al fine di ridurre i falsi negativi, la soluzione di *Vulnerability Assessment* deve essere integrata con *Data Feed* di *Intelligence* aggiornati con frequenza almeno giornaliera.

Criterio di valutazione della soluzione individuata è la frequenza delle analisi previste in fase di pianificazione, prediligendo soluzioni che siano in grado di eseguire il *monitoring* continuativo del livello di rischio di una infrastruttura, andando a simulare attacchi reali complessi (esempio: *Ransomware*) in **modalità supervisionata per le fasi critiche,** quali *exploiting* e *pivoting*, ed effettuando il *cracking* di eventuali *hash* di *password* intercettate durante le analisi.

Le analisi devono produrre risultati che esprimano il rischio tramite *standard* **CVSS** e identifichino le vulnerabilità tramite *standard* **CVE**.

I ***Penetration Test*** devono essere eseguiti da personale che abbia contribuito alla messa in sicurezza di soluzioni presenti sul mercato e *open source*, dunque che abbia scoperto e pubblicato vulnerabilità di tipo **0day**.
Infine, tutte le attività di *Security Assessment* devono essere eseguite da **personale certificato**.

Le attività di *Security Assessment* devono essere applicate a tutti gli elementi costituenti la PNT, dunque, devono essere previsti *Security Assessment*, sui canali di comunicazione *Wireless* ***Wi-Fi*** **e** ***Bluetooth*** e sulle componenti ***hardware***.

4.1.4.1. Threat Modeling

Al fine di identificare le possibili minacce che il sistema potrebbe essere chiamato ad affrontare - e, quindi, al fine di ridurre, o eliminare, l'esposizione a potenziali debolezze -, è richiesta l'esecuzione del *Threat Modeling*.

Il risultato dell'attività di *Threat Modeling* deve essere sintetizzato in un documento (*Report* di *Threat Modeling*) suddiviso in due sezioni: nella prima, minacce e problemi di sicurezza riscontrati, valutazione dei rischi in relazione alle conseguenze (impatti) e alla probabilità di accadimento; nella seconda, i principali requisiti che devono essere attivati per arginare i potenziali problemi di sicurezza.

L'obiettivo è identificare, elencare e classificare le minacce potenziali, le vulnerabilità strutturali o l'assenza, al momento dell'analisi, di misure di sicurezza adeguate.

Lo scopo della modellazione delle minacce deve essere in grado di fornire un'analisi sistematica di quali controlli, o difese, debbano essere previsti,

tenendo conto della natura del sistema, dei vettori di attacco più probabili e delle risorse più "desiderate" da un attaccante.

Questo passaggio deve essere eseguito in fase di disegno dell'Architettura del *software*, in conformità con i requisiti specificati nella precedente fase di analisi, in particolare per le scelte dei meccanismi di autenticazione, autorizzazione, riservatezza e non ripudio dei dati gestiti dal sistema.

Il processo di *Risk Management* da adottare nel Sistema di Gestione della Sicurezza ISO27001 si dovrà applicare, in generale, a tutti i processi di *business* aziendali per la realizzazione dei prodotti/servizi, anche, in termini di approccio, per quelle aree che non rientrano, strettamente, nell'ambito della certificazione ISO.
L'analisi va integrata nel processo di *Risk Management* adottato nel Sistema di Gestione della Sicurezza ISO27001.

4.1.4.2. DevSecOps

Deve essere analizzato il codice sorgente mediante attività di *Code Review*, al fine di rilevare vulnerabilità introdotte in fase di sviluppo.
Devono essere verificati e validati principalmente:

- i meccanismi di autenticazione e autorizzazione degli utenti;
- i meccanismi di validazione ed integrità del dato destinato ad essere processato sia *server*, che *client side*;
- i segmenti critici di codice che potrebbero causare errori e disservizi nell'esercizio dell'applicazione.

Le analisi e la reportistica sono eseguite in maniera automatizzata ed integrata nel processo *DevSecOps*. Pertanto, deve essere previsto un sistema intermedio di micro-validazione che consenta di validare i micro-rilasci.
Oltre a sottoporre ad analisi il codice sorgente mediante attività di *Static Application Security Testing* (SAST), gli applicativi devono essere sottoposti a *Dynamic Application Security Testing* (DAST), in maniera analoga, integrata nei processi di DevSecOps, al fine di delineare una visione completa dei seguenti aspetti:

- rilevare e testare i difetti e/o vulnerabilità presenti nel codice sorgente dell'applicazione;
- rilevare consumi eccessivi di risorse;
- identificare eventuali errori di programmazione (*null point*, *memory leaks*, *race conditions*);
- rilevare difetti di progettazione e di implementazione (coerenza di struttura in tutto il codice che la compone);

- analizzare i potenziali scenari e vettori di attacco, da fonti sia di natura esterna che interna, offrendo, così, una panoramica dei problemi di sicurezza dell'applicazione estremamente dettagliata e indicando le opportune modifiche al codice, a fini di mitigazione e prevenzione;
- identificare i rischi esistenti e l'annesso livello di rischio e calcolarne l'impatto su sistemi, servizi ed attori, a supporto dei processi decisionali in tematiche relative alla strategia di sicurezza e gestione dei rischi;
- indicare chiari e precisi interventi volti alla mitigazione o completa risoluzione delle criticità individuate in *step* precedenti.

4.2. Sistema di Gestione della Sicurezza delle Informazioni (SGSI)

La PNT deve prevedere l'instaurazione di un adeguato sistema di gestione della sicurezza delle informazioni ("SGSI"), consistente in un processo iterativo articolato in successive implementazioni, monitoraggi e successive fasi di riesame e miglioramento.
Il perimetro di validità del SGSI è quello individuato dai dati gestiti dalla Piattaforma e dalle risorse e strumenti ad essa afferenti, gestiti dalla PNT stessa relativamente all'erogazione dei servizi.
La PNT deve adottare il proprio SGSI in relazione alle specifiche espresse nel presente PTAS e in considerazione degli *standard* e della normativa di riferimento. La documentazione di attuazione del SGSI prodotta deve essere mantenuta, costantemente, aggiornata in relazione alle successive evoluzioni del sistema.
La documentazione inerente il SGSI deve essere gestita in modo da assicurarne il livello di protezione adeguato. Per tale documentazione, il Concessionario deve definire e attuare una procedura che definisca le azioni di gestione necessarie a:

- riesaminare ed aggiornare i documenti e riapprovare i documenti in caso di modifiche successive;
- assicurarsi che siano identificati i cambiamenti e l'attuale stato di revisione dei documenti;
- assicurarsi che le versioni più recenti dei documenti rilevanti siano facilmente identificabili e disponibili, prevenendo l'utilizzo non intenzionale di documenti obsoleti;
- assicurarsi che la distribuzione dei documenti sia controllata.

Il Concessionario deve predisporre gli strumenti e processi di gestione della documentazione opportuni, al fine di garantire la conservazione e l'aggiornamento della documentazione di sistema.

Il Concessionario deve, in particolare, produrre e rendere disponibili all'Amministrazione, entro 60 (sessanta) giorni dall'avvio delle attività della Concessione, i seguenti documenti:

- Documento di gestione delle registrazioni che forniscono evidenza della conformità ai requisiti e dell'efficace operatività del SGSI;
- Programma e procedura di *audit*;
- *Template* campi del Registro delle azioni per la registrazione di ogni incidente e/o rilievo di *audit*;
- Processo di *Incident Management* e criteri di classificazione degli incidenti di sicurezza;
- *Template* per il riesame del SGSI;
- Valutazione dei rischi;
- Modulo di *reporting* per le analisi periodiche di Incidenti, Criticità e Malfunzionamenti;
- Piano di Sicurezza, in cui deve descrivere approfonditamente le modalità logistiche ed organizzative, gli strumenti e i sistemi che intende adottare o di cui è provvisto per rendere sicuro e protetto l'ambiente da cui avviene l'erogazione dei servizi e in cui sono ospitati i dati.

Tali documenti devono essere mantenuti aggiornati dal Concessionario mediante una attività di revisione almeno annuale con una modalità da concordare con il Concedente in fase di avvio delle attività.

4.3. Protezione dei dati e dell'infrastruttura

4.3.1. *Analisi perimetrale avanzata*

La protezione della Piattaforma, oltre ai consueti sistemi di protezione perimetrale (*firewall*, IDS, IPS, ecc.), deve prevedere servizi che consentano la gestione della superficie di attacco ("***Attack Surface Management***") che, tramite una metodologia passiva e *agentless*, possa sottoporre ad analisi e monitoraggio ogni soggetto coinvolto attivamente e direttamente nell'erogazione del Servizio.

Per l'identificazione di elementi, che necessitino di approfondimenti, deve essere prevista l'attivazione di interventi di ***Threat Intelligence***, che consentano di ottenere analisi dettagliate delle minacce sia su scala globale, sia nel panorama italiano. In ogni caso, le informazioni devono essere in italiano.

Durante l'intera durata dell'erogazione del Servizio, deve essere attivo un sistema di *Threat Intelligence* che sia in grado di analizzare la ***Supply Chain*** (catena dei fornitori) e rilevare ogni possibile **minaccia esterna *cyber*** relativa l'organizzazione che ne fruisce.

La soluzione individuata per la PNT deve prevedere una componente in grado di analizzare la catena dei fornitori, in modo da indicare i rischi di compromissione dei dati e/o dell'infrastruttura, tramite una conseguenziale e potenziale violazione subita dai fornitori/attori terzi.

La soluzione deve generare un punteggio complessivo per indicare la classe di rischio del soggetto fruitore e devono essere disponibili grafici e informazioni che consentano una visione globale di tutte i soggetti fruitori, del gruppo e di dettaglio di ogni soggetto.
I grafici devono essere interattivi e consentire la navigazione dell'informazione, sino ad un livello granulare di dettaglio.
Le informazioni rappresentate devono essere relative sia ad uno specifico soggetto, sia ai soggetti della *supply chain*, mostrando una cronologia dell'andamento del livello di sicurezza di ogni soggetto fruitore.

La soluzione deve enumerare gli *asset* del soggetto fruitore, in modalità passiva, siano essi *asset* associati ad uno specifico soggetto, appartenenti alla sua *Supply Chain* o *Shadow IT*, a partire dalla ragione sociale, senza necessità di specificare dati tecnici, quali ad esempio IP, ASN, URL, ecc.
Gli *asset* rilevati devono essere geolocalizzati e mostrati su una mappa mondiale e, per ogni *asset*, deve essere indicato se questo è stato compromesso e indicare le evidenze.

Per ogni *asset* rilevato deve essere indicato il grado di fiducia di associazione ad un determinato soggetto e deve essere riportato IP, FQDN, porte e servizi rilevati.

Per ogni FQDN devono essere enumerati, in modalità passiva, tutti i certificati disponibili, con le relative date di validità e *common name*, consentendo, opzionalmente, di eliminare i falsi positivi abilitando la modalità attività.

Per ogni *asset*, deve essere indicato se è ragionevole supporre si tratti di *Phishing* o *Shadow* IT e, se presente un MX *server*, indicare lo stato dell'SPF, del DMARC e del rDNS.

Deve essere possibile effettuare l'*export* dei dati in formati compatibili con i fogli di calcolo e consentire l'*import* di una lista di *account* di posta elettronica al fine di verificare, per ogni *account*, la presenza di informazioni nei *data breach*.

Devono essere monitorate le minacce globali, così da fornirne una rappresentazione grafica per i responsabili ed una rappresentazione di dettaglio per gli utenti operativi, consentendo una contestualizzazione delle minacce in un determinato lasso di tempo.

Le informazioni devono essere classificate mediante *Traffic Light Protocol* ("TLP").
I *Threat Actor* (o Avversari) devono essere sottoposti a monitoraggio, principalmente tramite i canali di comunicazione generalmente utilizzati da quest'ultimi.

La soluzione deve prevedere un processo che consenta la rimozione automatizzata dei contenuti riservati sui siti di terze parti contenenti eventuali *data leak*.

Al fine di proteggere gli utenti della Piattaforma, i principali siti *web* correlati devono essere sottoposti a monitoraggio almeno giornaliero per rilevare potenziali minacce veicolate tramite codici offuscati, *malware* javascript o altri elementi malevoli *web-based*.

4.3.1.1. Takedown

Per fronteggiare minacce provenienti dal *Deep* e *Dark Web*, deve essere attivata una soluzione di *Takedown* che sia in grado di tracciare ogni azione, raccogliere e archiviare le evidenze delle minacce, fornire aggiornamenti (*follow-up*), dunque monitoraggio finalizzato a rilevare, e segnalare, l'eventuale riattivazione della minaccia, la completa disattivazione o l'eventuale migrazione della stessa.

I *Takedown* devono avvenire su ogni livello possibile relativo alla risorsa gestita dal *Threat Actor*, ad esempio a livello sia IP, sia DNS.

4.3.2. Log Management/SIEM

La raccolta e la conservazione degli eventi generati dalla Piattaforma e registrati sui *log* di sicurezza deve essere demandata ad un sistema dedicato di *Log Management* con funzionalità di SIEM.
La raccolta degli eventi deve garantire la conformità al Provvedimento del Garante Privacy per gli Amministratori di Sistema. A questo riguardo, devono essere considerati nell'ambito del *Log Management* i sistemi utilizzati negli ambienti di produzione, estendibile ai sistemi di certificazione, qualora espressamente richiesti dall'Amministrazione.

Il sistema di *Log Management* deve essere in grado di raccogliere e organizzare i dati relativi alla sicurezza in un unico punto di controllo e gestione. La funzionalità di SIEM resa disponibile deve poter individuare segnali critici, attraverso l'analisi dei dati contenuti nei *log* di sicurezza, e permettere di inviare comunicazioni di allerta ad un *team* di *Cybersecurity* che si occupa della gestione operativa; quest'ultimo è, così, in grado di reagire e rispondere agli attacchi indirizzati al sistema e/o all'applicazione.
Il sistema deve essere in grado di ricevere dati da un parco tecnologico eterogeneo (i sistemi ed i componenti infrastrutturali facenti parte della piattaforma PNT), correlandoli per massimizzare la rilevazione di anomalie e attacchi e per garantire i livelli di sicurezza mediante le regole configurate. Il SIEM deve, quindi, effettuare un'analisi proattiva di tutti gli eventi, al fine di identificare anomalie, attacchi e/o comportamenti potenzialmente fraudolenti.
Più in generale, il sistema SIEM deve consentire:

- la raccolta e la normalizzazione dei dati registrati sui *log* di sicurezza;
- il *data mining* e la correlazione (identifica schemi di minacce e monitora l'evoluzione degli incidenti evidenziando attacchi di per sé non evidenti dall'analisi dei singoli eventi);
- l'analisi di eventi e *alerting* (quantificare gli incidenti, scartare i falsi positivi e segnalare possibili incidenti);
- *event* reporting di sicurezza.

4.3.3. *Advanced Endpoint Protection*

Il servizio *Advanced Endpoint Protection* ha lo scopo di fornire una soluzione per la **protezione avanzata dei *server* fisici e virtuali**. Deve consentire l'installazione e gestione in ambienti eterogenei attraverso la gestione automatizzata di *policy*, sicurezza *agentless hypervisor-integrated*, *agent-based*, o mista.
Il servizio si deve basare su tecnologie che prevedono meccanismi di **protezione** da minacce di ***malware***, quali ***ransomware***, da attacchi di *cryptocurrency mining* e attacchi *network-based* anche su canali SSL. A queste caratteristiche, si aggiungono le funzionalità di ***Virtual Patching*** ed ***IDS/IPS***, che proteggono l'*endpoint* dalle vulnerabilità di *software* obsoleti, o per le quali non è possibile applicare una *patch*. Deve, inoltre, prevedere funzionalità di *Host Based Firewall*, in grado di definire *policy* per i protocolli e le porte ammessi in ingresso ed in uscita.

Il servizio deve prevedere che le verifiche di sicurezza di contenuti eseguibili possano essere inoltrate ad un sistema di ***sandboxing***, in grado di "*detonare*"

l'elemento analizzato in un ambiente protetto, al fine di identificarne il comportamento malevolo e prevenirlo.

4.3.4. *Web Application Firewall*

Il servizio di *Web Application Firewall* ("WAF"), necessario per la protezione perimetrale delle applicazioni *Web* erogate, deve essere erogato su servizi *cloud*.

Il WAF deve consentire il controllo granulare delle richieste effettuate su protocollo http/https (URL, *form*, *cookie*, *query string*, *hidden field* e parametri) verso l'applicazione, per individuare eventuali possibili minacce all'applicazione ed eventualmente bloccare la richiesta malevola. Il WAF consente, quindi, di proteggere l'applicazione da minacce esterne, rilevando e mitigando l'eventuale *exploiting* di vulnerabilità che possono essere presenti nel codice dell'applicazione, nelle librerie/*plug-in* di terze parti o nelle API.

Il servizio di WAF deve prevedere la possibilità di ***malware prevention***, finalizzata alla identificazione ed al blocco di *malware* in transito.

Il servizio WAF deve, inoltre, consentire di aggiungere le funzionalità di *Content Delivery Network* (CDN) e AntiDDoS al fine da garantire un ulteriore *layer* di protezione contro attacchi di tipo distribuito e volumetrico. Il servizio AntiDDoS deve essere erogato mediante un'architettura *cloud* connessa con CDN dedicata ai sistemi da esporre sulla rete, che permetta di proteggerli da possibili attacchi DDoS che, basandosi sulla generazione di un quantitativo enorme di traffico, potrebbero tentare di rendere il sistema non raggiungibile. L'uso di una soluzione basata sul *Cloud* permette di sfruttare le naturali caratteristiche di resilienza di tale infrastruttura, lasciando inalterata l'infrastruttura di effettiva erogazione del servizio.

Il WAF deve essere integrato con la piattaforma di SIEM per una gestione integrata delle segnalazioni.

4.3.5. *Data Encryption*

4.3.5.1. *Cifratura dei dati*

Al fine di rispettare i principi di protezione dei dati, è necessario prevedere soluzioni di *encryption* che coprano tutti i livelli del sistema, dalla cifratura dei dati ***at-rest*** (quando ospitati su uno *storage*) fino alla gestione ***in-transit*** (quando i dati sono trasmessi), eventualmente anche prevedendo livelli di protezione molteplici.

Il sistema individuato per la PNT deve rendere disponibile una soluzione di KSM (*hardware* o *software*), destinato ad ospitare le chiavi di cifratura usate.

È richiesto che gli algoritmi usati per la cifratura siano *standard* e basati su tecnologie *open-source*.
Si richiede, inoltre, che la soluzione preveda l'uso di metodologie di cifratura in grado di limitare l'accesso ai dati decifrati ai sistemi ed agli utenti; tra questi, ci si attende l'uso di soluzioni di cifratura basate su algoritmi che permettano il trattamento cifrato del dato senza necessità della decifratura (per esempio la *Format Preserving Encryption*).
Parallelamente, devono essere gestite soluzioni di cifratura convenzionali (tipicamente protocolli HTTPS e SSL) per l'accesso a tutti i servizi della Piattaforma.
I dati dell'applicazione memorizzati nei *database/filesystem* devono essere cifrati tramite algoritmi simmetrici. Inoltre, per i dati di natura critica, oltre che la cifratura, deve essere previsto l'utilizzo di strumenti che garantiscano la possibilità di vagliarne integrità e autenticità (es. utilizzo di algoritmi di *hashing* o apposizione della firma digitale).

4.3.5.2. Key Server e gestione delle chiavi

Il sistema deve prevedere una soluzione di gestione delle chiavi sicura basata su KSM o HSM.
Le politiche di gestione delle chiavi possono prevedere l'uso di soluzioni di *key server* basati sulla tecnologia dello *Stateless Key Management*, tale da permette di generare *on-demand* tutte le chiavi di cifratura e decifratura necessarie, senza la necessità di archiviare, o effettuare *backup* dell'archivio delle chiavi.
Per tutti i sistemi di gestione delle chiavi, devono essere garantiti livelli adeguati di alta affidabilità, alta disponibilità, bilanciamento e resilienza.

4.3.6. Gestione dei Certificati SSL/TSL

Il servizio deve gestire il ciclo di vita dei certificati digitali emessi sia da *Certification Authority* pubbliche, che private.
L'esposizione di sistemi/applicazioni su Internet deve prevedere la pubblicazione attraverso l'utilizzo di certificati digitali emessi, esclusivamente, da *Certification Authority* pubbliche.
Per l'eventuale esposizione dei sistemi che avvenga non su rete pubblica, ma sulla intranet della Piattaforma, possono essere utilizzati certificati emessi da *Certification Authority* private.

4.3.7. Gestione Incidenti di sicurezza

L'obiettivo del processo di "*Gestione Incidenti di Sicurezza*" è di prevenire, intervenire e ripristinare le operazioni normali di servizio il più velocemente

possibile, con la minima interruzione di servizio al *business*, assicurando alti livelli di servizio e di disponibilità e la *compliance* con l'art. 33 del GDPR.

Il servizio di "*Gestione Incidenti di Sicurezza*" deve, dunque, identificare, in maniera preventiva, le minacce e gli elementi di rischio che potrebbero essere causa di un incidente, minimizzandone l'impatto sulle informazioni gestite.
Le attività previste nel processo adottato devono prevedere:

- rilevazione e identificazione dell'Incidente;
- classificazione del livello di criticità;
- notifica ed *escalation*;
- *recovery*;
- *follow-up* & *Incident report*.

4.3.8. Agenzia per la Cybersicurezza Nazionale ("ACN")

Nell'ambito delle analisi perimetrali avanzate, sfruttando un servizio di *Threat Intelligence*, la soluzione identificata per la Piattaforma deve prevedere una collaborazione automatizzata con l'ACN, acquisendo informazioni relative alle principali minacce a cui le organizzazioni italiane sono esposte.
Le informazioni acquisite devono essere classificate in base a diversi livelli di rischio, arricchiti con indicatori in grado di determinare eventuali stati di compromissione dei sistemi, e, conseguentemente, le azioni di mitigazione necessarie per la gestione delle minacce.

4.3.9. Sistema di *Advanced Fraud Detection*

La varietà, la velocità ed il volume dei dati prodotti dai servizi prestazionali offerti dalla Piattaforma generano un'evoluzione esponenziale della complessità della natura dei fenomeni che il sistema deve essere in grado di monitorare e gestire.
Comportamenti che si distanziano dagli *standard*, anomali, eventualmente fraudolenti sono sempre più difficili da intercettare con sistemi basati su regole predeterminate. Oltre alla complessità numerica e fenomenologica, si deve prevedere anche una mutevolezza degli eventi, che potrebbe rendere sempre più inefficace un monitoraggio solo deterministico e, di converso, sempre più fondamentale un'integrazione con sistemi di analisi avanzata, capaci di scoprire *pattern* anomali non evidenti, o, addirittura, nuovi, sfruttando soluzioni di ML ed apprendimento automatico.
A tale scopo, la Piattaforma deve essere dotata di una componente applicativa che sia in grado di raccogliere e normalizzare, nel tempo, i dati relativi alle prestazioni di telemedicina erogate. Dopo una prima fase di raccolta, la componente deve riconoscere i gruppi di similarità tra i dati delle

prestazioni sui quali, poi, applicare tecniche non-supervisionate per individuare dei *trend* o stati "*normali*" ed **evidenziare punti isolati, anomali che possono significare attività fraudolente o malevole**.
Il sistema deve consentire il tracciamento delle azioni svolte, sia in termini di utilizzo della Piattaforma, che rispetto ad eventuali trasformazioni operate sui dati.
La funzionalità deve esprimere garantire maturità e solidità che permetta la produzione di segnalazioni efficaci ed in grado di evolvere nel tempo automaticamente con logiche di auto addestramento.

4.4. Identity and Access Management

Il servizio di "*Identity & Access Management*" ("IAM") deve essere erogato mediante una soluzione tecnologica centralizzata, che consenta la realizzazione dei servizi nel rispetto dei maggiori *standard* di sicurezza e in linea con lo stato dell'arte della tecnologia.

L'architettura della soluzione deve adottare i seguenti paradigmi:

- ✓ *Software Open Source*
- ✓ Architettura a microservizi
- ✓ Docker *container*
- ✓ *Multi-tenancy.*

La soluzione adottata si deve configurare in modalità *Security as a Service* per i servizi di autenticazione, autorizzazione e gestione delle identità digitali mediante un'architettura IaaS.

I servizi IAM da erogare sono:

a) gestione delle identità digitali e del ciclo di vita delle utenze e delle credenziali degli utenti, in accordo con i processi definiti dal committente;
b) autenticazione e controllo della sicurezza degli accessi logici degli utenti, in accordo con le politiche di sicurezza del committente;
c) conduzione tecnica ed applicativa della soluzione IAM;
d) supporto specialistico di secondo livello per l'analisi e la risoluzione delle problematiche;
e) predisposizione della documentazione e della reportistica del servizio.

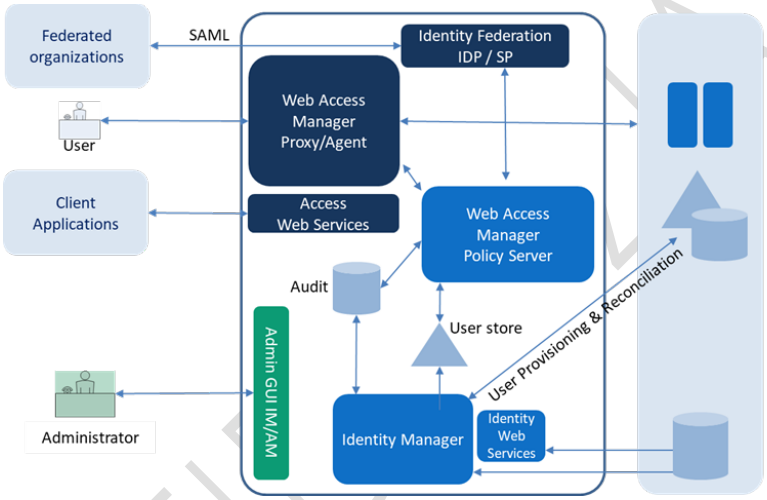
Il sistema IAM deve prevedere due sottosistemi scalabili (AM e IM), integrati tra loro, ossia:

a) controllo accessi/*Access Management* (AM),

b) gestione degli utenti/*Identity Management* (IM).

Con l'integrazione dei due sottosistemi, deve essere garantita l'erogazione delle seguenti funzionalità:

a) *Web Access Manager;*
b) *User Provisioning*;
c) *Role Management*;
d) *Federation*;
e) *Web Service Security*.



4.4.1. *Access Management* (AM)

La componente AM deve offrire la possibilità di utilizzare vari fattori di autenticazione (es. Nome / Password, X.509, ecc.), anche in cascata, tra cui: HOTP e TOTP (per la richiesta di OTP generate da *App Authenticator*), *SecureID*, *Windows Desktop SSO* (*Kerberos*/NTLMv2), *Radius*.
Deve essere prevista la **federazione con gli *Identity Provider* SPID**, nonché l'abilitazione del Committente come ***Service Provider* SPID**. Inoltre, tramite il protocollo XACML, la soluzione deve supportare anche l'implementazione **dell'entità SPID *Attribute Authority***.

Al fine di garantire **l'integrazione con altri sistemi informatici** (es. *Active Directory*, LDAP vari), la soluzione deve essere pienamente *compliant* alle specifiche tecniche previste da AGID per il protocollo SAML 2.0 e supportare i protocolli OAuth2/Open ID Connect.

È auspicabile la fornitura di un *Gateway* SPID, CNS, CIE che consenta all'Amministrazione di accreditarsi come "*Aggregatore di Servizi*" presso AGID.

Nello specifico, il *Gateway* deve prevedere un'interfaccia per l'autenticazione ai servizi con:

- ✓ SPID
- ✓ eIDAS *electronic IDentification Authentication and Signature*
- ✓ CIE
- ✓ CNS Carta Nazionale dei Servizi.

4.4.2. *Identity Management* (IM)

La componente IM deve gestire l'intero ciclo di vita, e relativi processi di *onboarding/offboarding*, per:

- ✓ identità digitali degli utenti previsti,
- ✓ *account* correlati sulle risorse aziendali (sistemi *target*),
- ✓ *device* di telemedicina.

Nel rispetto dei processi di identificazione e delle *policy* di sicurezza, occorre prevedere:

a) integrazione con le fonti autoritative del Sistema Informativo dell'Amministrazione;
b) integrazione con i processi amministrativi e con i *workflow* di gestione del personale e di assegnazione dei ruoli per gli aspetti che riguardano i privilegi di accesso alle risorse del Sistema Informativo del Committente;
c) *enrollment* con possibilità, ove applicabile, di invio di *QR code* per la configurazione automatica di *Mobile App Authenticator* OATH TOTP (Google, Microsoft, etc.), notifiche *push* e via SMS;
d) gestione delle richieste di *self-service* (recupero *password*, *reset password*) dal portale e anche direttamente dalle postazioni windows.

La componente IM, come la componente AM, deve utilizzare *standard* e *framework Open Source*. Nell'ambito dei *web service*, la componente IM deve esporre un'interfaccia di programmazione (Rest e SOAP) per le applicazioni che hanno necessità di reperire ed utilizzare le informazioni relative agli utenti e la relativa profilatura.

Per l'interfacciamento con le risorse esterne al sistema PNT, per consentire la propagazione degli *account* utenti (*provisioning*), la componente IM deve prevedere un approccio modulare e di adeguati meccanismi di autenticazione basati su connettori "*agentless*" o di tipo "*agent*".

4.4.3. Modello di Profilazione

Le regole di gestione degli utenti, dei privilegi e delle risorse devono essere analizzate e individuate fino al massimo livello di dettaglio possibile, nella specifica realtà organizzativa.

La soluzione IAM deve poter adottare diversi modelli di profilazione:

- ✓ Modello *Role-Based Access Control* (RBAC).
- ✓ Modello *Attribute-Based Access Control* (ABAC), XACML
- ✓ Modello Utenza-profilo.

Devono essere garantiti i principi del privilegio minimo necessario e il principio della separazione delle responsabilità (*Segregation of Duties*).

5. Assetto Transitorio

Il presente PTAS preconizza la piena aderenza alle progettualità nazionali ed in particolare al nuovo FSE.

Nella predisposizione del presente documento è posta particolare attenzione al documento "*Piattaforma di Telemedicina ed Ecosistema FSE - Punti di contatto e raccordo tra i due progetti*" ed alle Linee Guida per l'Attuazione del Fascicolo Sanitario Elettronico, pubblicate in G.U. n. 160 del 11/07/2022 (le "Linee Guida FSE").

I nuovi elementi che vanno a completare l'architettura del Fascicolo Sanitario Elettronico sono il *Gateway*, o GW e l'Ecosistema dei Dati Sanitari, o EDS.

Nelle succitate Linee Guida FSE, a proposito di "*Servizi di Telemedicina*", si legge che essi:

- alimenteranno il *Data Repository* (facente parte dell'EDS) con i dati acquisiti dai dispositivi medici, e
- lo consulteranno per accedere ai dati clinici degli assistiti presi in carico.

Inoltre, a proposito di "*Casa come primo luogo di cura e telemedicina*", sempre nelle **"Linee Guida FSE"** si afferma che "***il FSE deve integrarsi con i servizi di telemedicina [...] sia al fine di acquisire dati da essi rilevati, che di mettere a disposizione dati clinici degli assistiti presi in carico nell'ambito di tali servizi.***".

In questo contesto di progettualità fortemente interconnesse (FSE e PNT) ed in riferimento alla necessità di garantire il *target* previsto per la PNT, ovvero l'avvio entro novembre 2023, è necessario prevedere un eventuale Assetto Transitorio, ossia un *set* minimo di servizi, garantiti a regime dal EDS e dal GW, che possano permettere, in ogni caso, la piena funzionalità della PNT, anche ove GW e/o EDS non siano ancora, a quella data, pienamente operativi.

L'Assetto Transitorio permette, dunque, ove necessario, di istanziare centralmente ed in modo indipendente il modulo *Gateway* (GW Transitorio) ed il modulo EDS (EDS Transitorio).

Il GW Transitorio deve mettere a disposizione un *set* minimo di funzionalità, in particolare con l'attivazione a livello di nodo centrale di istanze regionali, che devono consentire l'acquisizione dei dati e dei documenti dai sistemi

legacy delle strutture sanitarie ed il loro invio al *repository* una volta che siano stati "tradotti" in formato HL7 FHIR (se non nativamente già prodotti in questo standard). Il GW Transitorio deve anche prevedere un meccanismo di validazione sintattica e semantica dei dati e dei documenti.
Operando con lo standard HL7 FHIR e con le logiche descritte dalle già menzionate Linee Guida, nel momento in cui il FSE mette a disposizione il GW, si può immaginare che, una volta testato il corretto funzionamento della PNT con il GW nazionale, il GW Transitorio può essere disattivato, congiuntamente alle istanze regionali.

Nel caso del EDS Transitorio (basato su HL7 FHIR), il *set* minimo deve contenere il *Data Repository* Transitorio, che registra i dati provenienti da sistemi di telemedicina ed eventualmente anche tutti i dati clinici (provenienti dai sistemi o autonomamente generati dagli utenti) utili agli scopi della PNT. L'EDS Transitorio è alimentato per il tramite del GW (nazionale o transitorio) e consente di realizzare meccanismi di interoperabilità dei dati tra regioni. È necessario, comunque, prevedere meccanismi di indicizzazione del dato, per evitare fenomeni di duplicazione o rendere inefficace la interoperabilità a livello nazionale.
Una volta attivato l'EDS nazionale, deve essere prevista una attività di migrazione dei dati presenti nel EDS Transitorio e, successivamente alla verifica del pieno funzionamento, quest'ultimo può essere disattivato.

In fase di predisposizione della Progettazione di Dettaglio, è necessario verificare i processi attuativi del GW e dell'EDS e, congiuntamente all'Amministrazione, procedere con l'eventuale predisposizione della progettualità di dettaglio inerente al GW Transitorio o all'EDS Transitorio o ad entrambi.

Tale attività è ricompresa, come meglio declinato nel capitolo 7 del PTAS, nella fase di progettazione (facente parte della Fase di Start Up) ed ha come *output* la eventuale proposta all'Amministrazione di esercitare l'opzione prevista contrattualmente ed attivare il GW Transitorio, o l'EDS Transitorio, o entrambi, compresa la progettazione di dettaglio delle suddette componenti e della interazione sia con la PNT, che con l'evoluzione della realizzazione del FSE.

La realizzazione dell'Assetto Transitorio, così come definito a livello di Progettazione di Dettaglio, può avvenire contemporaneamente alla realizzazione della PNT, mediante *team* distinti, vista la sua natura opzionale e non ricompresa tra le attività incluse nel PEF.

Nella progettualità relativa all'Assetto Transitorio deve essere prevista la fase di *phase out* con le attività che devono essere attuate per non impattare nelle funzionalità e nella disponibilità della PNT.

6. Assunzioni e dimensionamenti

La Piattaforma di cui al PTAS è interamente e nativamente *cloud*, in aderenza alle strategie nazionali.

La Piattaforma prevede un nodo centrale *multi-tenant*, che garantisce la capacità di poter servire con un livello di isolamento adeguato servizi centrali, per le singole regioni e specifiche AASS, nonché un numero di singole viste in funzione degli attori che sono coinvolti nella PNT o in funzione dell'attivazione di istanze qualora sia necessaria (i.e. nel caso del c.d. Assetto Transitorio).

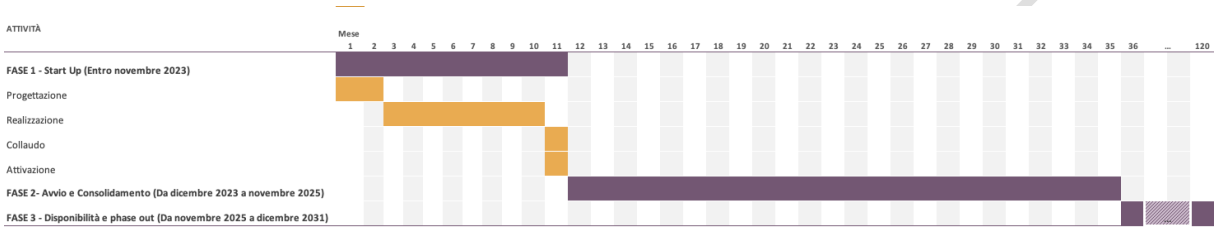
La PNT deve essere oggetto di evoluzioni che ne garantiscono la aderenza con gli obiettivi dell'Amministrazione e il continuo aggiornamento tecnologico. Tali evoluzioni sono ricomprese nel canone di periodo (di avvio e consolidamento per i primi due anni, di disponibilità dal terzo anno). Tale approccio garantisce che la Piattaforma rappresenti sempre lo stato dell'arte e possa seguire le evoluzioni previste da altri progetti nazionali, con cui condivide taluni obiettivi, primo tra tutti il FSE 2.0.

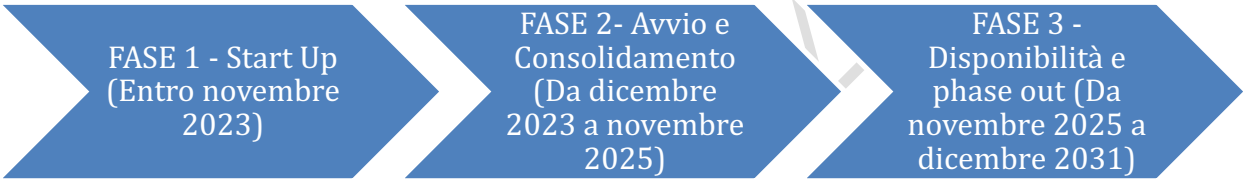
Devono essere previste attività professionali per il supporto alla creazione di cruscotti o all'analisi dei dati raccolti, per il supporto alla validazione di soluzioni di telemedicina ed il successivo *onboarding* nella PNT. Le attività professionali sono garantite dalla attivazione della PNT fino alla conclusione della Concessione e sono parte integrante (unitamente al personale relativo all'*application operation*) del *know-how* che gli operatori economici si devono impegnare a trasferire al nuovo gestore della PNT al termine della Concessione.

Il numero di accessi garantiti dalla infrastruttura in un arco temporale di 5 minuti deve essere pari ad almeno 200.000 utenze. Il dimensionamento della Piattaforma è, pienamente, conforme alla popolazione che utilizza ed accede sia al SSN, che ai vari SSR. Per la stima suddetta, nel contesto della PNT, si è fatto riferimento a processi simili a quelli che caratterizzano altri servizi pubblici resi mediante piattaforme informatiche, considerando anche un probabile aumento dell'uso dei servizi, collegato alla sempre maggiore digitalizzazione dei cittadini nei prossimi anni ed ai processi di invecchiamento della popolazione italiana. Per la parte di acquisizione dati, la Piattaforma agisce in modo asincrono rispetto all'allineamento con gli altri sistemi nazionali e regionali.

7. Cronoprogramma

Questo capitolo descrive le principali fasi del progetto PNT e della loro iterazione con altre progettualità nazionali, rappresentate in modo sintetico dagli schemi che seguono:





7.1. Fase 1 - Start Up (Progettazione, Realizzazione, Collaudo ed Attivazione)

La fase di Start Up segue la firma della Convenzione, si avvia con la progettazione, prosegue con la realizzazione della Piattaforma e si conclude con il Collaudo e la relativa attivazione della PNT.

Dalla firma della Convenzione si avvia l'attività di progettazione: questa attività vede impegnato personale del Concessionario, con personale dell'Amministrazione e di quanti, individuati dall'Amministrazione stessa, sono parte in causa, per esempio personale che segue le progettualità nazionali come il FSE.

La progettazione di dettaglio deve essere completata entro 2 (due) mesi dalla firma della Convenzione e realizzata assicurando una forte interdipendenza con le altre progettualità nazionali, in particolare il FSE e, conseguentemente, con l'EDS ed il GW. In questa fase, è necessario verificare la necessità, o meno, di attivare il c.d. Assetto Transitorio o di adeguare le attività realizzative ad

eventuali indicazioni/prescrizioni/requisiti/funzionalità, che dovessero emergere dallo sviluppo, in parallelo, delle succitate progettualità nazionali.

Al termine di questa fase (entro la fine del Mese 2) si produce il documento denominato "Progettazione di Dettaglio", che contiene tutte le descrizioni relative alla Piattaforma sia dal punto di vista infrastrutturale, che dal punto di vista applicativo, con le iterazioni esterne e con l'eventuale attivazione dell'Assetto Transitorio (completo o parziale, come descritto nel Capitolo 5 del PTAS).

La Progettazione Esecutiva PNT deve contenere un capitolo relativo ai principi indicati dal PNRR e, in particolare, quello del DNSH, ossia che non arrechi un danno significativo all'ambiente. La PNT deve essere progettata per garantire elevatissima efficienza energetica e prevedere l'uso di energia prodotta al 100% da fonti rinnovabili. Per dimostrare l'impronta ambientale, la PNT deve prevedere l'uso di sistemi per il calcolo del *carbon footprint*, verificato e validato. Tale approccio deve consentire sia il calcolo degli impatti strettamente e direttamente connessi con le proprie attività, che quelli legati all'utilizzo, da parte degli utenti, di servizi di telemedicina (indiretti).

La progettazione di dettaglio deve essere sottoposta ad approvazione dell'Amministrazione. Essa può approvare il documento o richiederne modifiche. Al termine di questo processo, si avvia la fase di realizzazione della PNT.

La realizzazione della PNT, che prende avvio dalla accettazione della progettazione di dettaglio da parte dell'Amministrazione, deve essere completata entro 8 (otto) mesi.

Il Collaudo, con le modalità descritte nel Gestionale, si attiva al termine dello sviluppo e deve essere completato entro 45 giorni.

Al termine del positivo collaudo la PNT viene attivata.

L'attivazione della PNT dipende dal buon esito dei collaudi e, in ogni caso, deve essere completata entro novembre 2023, per questo deve essere posta in essere ogni azione che possa prevenire il non raggiungimento di tale termine.

Nel caso di non conformità, in sede di Collaudo di Avvio, è necessario effettuare più di una prova; quindi, l'avvio della fase di collaudo deve essere

tale da consentire l'eliminazione di ogni non conformità entro la suddetta scadenza.

Gli offerenti possono proporre soluzioni atte al contenimento del rischio di mancato raggiungimento dell'obiettivo posto.

7.2. Fase 2 – Avvio e Consolidamento

La Fase di Avvio e Consolidamento della PNT è successiva al Collaudo di Avvio dell'infrastruttura ed alla conseguente attivazione della Piattaforma e deve, in ogni caso, iniziare entro il 1° dicembre 2023.

Tale fase si conclude dopo 24 mesi e quindi entro il 30 novembre 2025.

In questa fase, a seguito delle attività di consolidamento descritte nel presente PTAS e nel Gestionale, è prevista una serie di nuovi rilasci dovuti sia alle attività di manutenzione adeguativa, che a quelle relative ai servizi professionali e l'*onboarding* di soluzioni di telemedicina nella PNT, relativamente ai processi di validazione, come descritte nel presente PTAS e nel Gestionale.

In questa fase, il Concessionario deve garantire, oltre che i servizi di governo della PNT, i servizi professionali di supporto all'Amministrazione sia per la realizzazione di cruscotti di *data analytic*, che per la validazione delle soluzioni di telemedicina e successivo *onboarding* delle stesse nella PNT.

Se si dovesse rendere necessario, dev'essere attivabile, su richiesta dell'Amministrazione, il processo di collaudo così come descritto nel Gestionale, per attività di manutenzione evolutiva e/o per quelle di predisposizione di cruscotti specifici su richiesta dell'Amministrazione.

7.3. Fase 3 – Disponibilità e *phase out*

La fase 3, ossia la Fase di Gestione a Regime o di Disponibilità della PNT, segue la conclusione del consolidamento e, quindi, prende avvio dal Verbale di Chiusura della Fase di Avvio e Consolidamento, entro il 1° dicembre 2025, e si conclude al termine della Concessione.

Sei mesi prima della scadenza della Concessione il Concessionario attiva la fase di *phase out*, ossia il passaggio della Piattaforma e dei relativi servizi al nuovo concessionario o alla Amministrazione.