# NUOVO SISTEMA PER LA GESTIONE DIGITALE DEL TERRITORIO

*INDICE*

# 1. Scopo del documento

Il presente documento è finalizzato a supportare la richiesta di Regione Lombardia di progettare e implementare un nuovo ecosistema digitale regionale per supportare l'erogazione dei servizi sociosanitari sul territorio. Il documento descrive i contenuti e le modalità proposte da ARIA spa  per la realizzazione del Sistema per la Gestione Digitale del Territorio.

# 2. Premessa e contesto di rifermento

Nel 2015, con l'approvazione della legge regionale n. 23 di "Evoluzione del sistema sociosanitario lombardo: modifiche al Titolo I e al Titolo II della legge regionale 30 dicembre 2009, n. 33 (Testo unico delle leggi regionali in materia di sanità)" Regione Lombardia ha inteso far evolvere le importanti capacità sviluppate nell'ambito ospedaliero anche nell'ambito dell'assistenza territoriale, superando alcune frammentazioni esistenti ed evitando le potenziali interruzioni nei percorsi di cura. L'individuazione di un unico soggetto deputato all'erogazione dei servizi sanitari e sociosanitari ha di fatto portato a compimento il principio di separazione delle attività di programmazione e controllo da quelle puramente erogative. Le previsioni introdotte con la legge regionale n. 23/2015 in materia di presa in carico dei pazienti affetti da patologie croniche e l'istituzione delle Aziende Socio-Sanitarie Territoriali, quali soggetti erogativi pubblici sia delle prestazioni ospedaliere (attraverso il Polo Ospedaliero) che delle prestazioni territoriali (mediante la Rete Territoriale), hanno rappresentato una forte innovazione rispetto alle previsioni del Decreto Legislativo n. 502/1992; in particolare l'istituzione di un soggetto giuridico nuovo e diverso rispetto alle Aziende Sanitarie Locali e alle Aziende Ospedaliere previste dal dettato normativo nazionale ha comportato la necessità di valutare sperimentalmente tale nuovo assetto organizzativo congiuntamente con il Ministero della Salute prevedendo un arco temporale di cinque anni.

A conclusione del quinquennio sperimentale, il Ministero della Salute ha analizzato con il supporto tecnico dell'Agenzia Nazionale per i Servizi Sanitari Regionali (Agenas) i risultati raggiunti con il nuovo assetto organizzativo. La valutazione di

Agenas ha messo in luce molti aspetti innovativi positivi apportati dalla legge regionale n. 23/2015, primo fra tutti i risultati di salute del modello di presa in carico dei pazienti cronici. Agenas ha tuttavia individuato alcune aree di miglioramento, la cui introduzione nell'assetto organizzativo del sistema sociosanitario lombardo è stata ritenuta indispensabile al fine di una valutazione positiva e coerente con il disegno nazionale delineato dal Decreto Legislativo n. 502/1992.

Durante la fase di valutazione della legge regionale n. 23/2015 e di conseguente avvio dell'iter di modifica normativa Regione Lombardia ha recepito le opportunità offerte dal nuovo fondamentale strumento di implementazione dei sistemi sanitari regionali, rappresentato dal Piano Nazionale di Ripresa e Resilienza (PNRR). La Missione 6 Salute PNRR, in particolare, promuove importanti interventi organizzativi e tecnologici attraverso i quali realizzare un modello di gestione dei servizi sociosanitari che rafforzi le prestazioni erogate sul territorio. Fornisce inoltre alcuni «requisiti» per lo sviluppo dei sistemi informativi, in particolare con riferimento alle Reti di prossimità e ai temi di Innovazione, ricerca e digitalizzazione del Servizio Sanitario Nazionale.

In questo scenario, il Progetto di Legge N. 0187 "Modifiche Al Titolo I e al Titolo VII della legge regionale 30 dicembre 2009, n.33 (Testo unico delle leggi regionali in materia di sanità)" approvato nella seduta del 27 ottobre 2021, ha definito gli obiettivi per l'evoluzione dell'assetto organizzativo del sistema sociosanitario lombardo, conformemente alle indicazioni di Agenas e del PNRR. Gli obbiettivi della L.0187 confermano infatti gli indirizzi nazionali e si basano sui principi di:1- Cura della Persona e non solo cura della malattia 2- Approccio One Health, che assicuri una *vision* complessiva della sanità, attraverso centri di prevenzione, ricerca e controllo; 3- Libertà di scelta del Cittadino ed equità di accesso alle cure.

Nella L.0187 viene potenziato per l'Assessorato al Welfare il ruolo di governo dell'ICT e viene posto l'obiettivo di potenziamento della rete territoriale tramite l'istituzione del distretto, quale luogo di integrazione tra tutti i professionisti sanitari e di coordinamento dell'offerta territoriale (Poliambulatori, COT, ospedali di comunità), l'attivazione di nuove strutture (sovrapponibili a quelle previste da PNRR) e il potenziamento dei servizi domiciliari.

# 3. Oggetto dell'iniziativa

In questo contesto di forte evoluzione degli scenari organizzativi, Regione Lombardia intende progettare e implementare un **nuovo ecosistema digitale regionale** per supportare l'erogazione dei servizi sociosanitari sul territorio e rendere disponibili strumenti informatici e tecnologie digitali per la gestione delle Case della Comunità e delle Centrali Operative Territoriali. L'ecosistema digitale è composto dai seguenti componenti principali:

- Sistema per la Gestione Digitale del Territorio: applicativo regionale per la gestione informatizzata dei processi sociosanitari del territorio e per la digitalizzazione di dati e documenti.
- Piattaforma Regionale di Telemedicina: architettura informatica per supportare e sostenere in modo strutturato e organizzato l'attuazione delle diverse tipologie di processi e servizi di Telemedicina.
- Architettura per la raccolta e valorizzazione dei dati distribuiti: modello architetturale basato su standard semantici per la raccolta, condivisione e utilizzo in tempo reale dei dati prodotti presso i diversi servizi sociosanitari di ambito ospedaliero e territoriale.

L'oggetto del progetto attuativo proposto da ARIAspa riguarda il **Sistema per la Gestione Digitale del Territorio**, che deve essere realizzato come soluzione applicativa unica e centralizzata messa a disposizione da Regione Lombardia per supportare gli Enti nell'attuazione dei processi sociosanitari integrati ospedale-territorio e nel concreto funzionamento delle Case della Comunità e delle Centrali Operative Territoriali.

Questi **processi** sono principalmente:

- Gestione del Punto Unico di Accesso (PUA) per l'accoglienza del paziente e la presa in carico delle situazioni di fragilità;
- Valutazione dei bisogni semplici e complessi;
- Definizione del Progetto Individuale;

- Attuazione del Progetto Individuale, attraverso l'attivazione dei nodi della rete sociosanitaria coinvolti, grazie al supporto della Centrale Operativa Territoriale (COT) per l'attivazione dei diversi servizi;
- Recepimento dei Piani di Assistenza Individuale (PAI) elaborati dai servizi sociosanitari attivati;
- Monitoraggio dell'attuazione del Progetto Individuale, attraverso la connessione con i sistemi dei gestori per recepire gli eventi e le informazioni correlate alla realizzazione dei PAI di struttura;
- Condivisione del diario multidisciplinare, strumento che riporta le attività eseguite dagli attori coinvolti.

Le caratteristiche del progetto attuativo, che sono dettagliate nel capitolo 7, sono riassumibili nei seguenti macro-elementi:

1. analisi, progettazione e sviluppo di **funzionalità applicative** del sistema per la Gestione Digitale del Territorio;
2. analisi, progettazione e sviluppo di **servizi di cooperazione applicativa** con i componenti dell'ecosistema regionale
3. implementazione delle **integrazioni al Sistema Informativo Socio-Sanitario Regionale SISS** di Regione Lombardia;
4. **servizi professionali** per supportare l'attuazione del progetto e la diffusione della trasformazione digitale dei processi per tutti gli Enti coinvolti (l'introduzione della soluzione negli enti richiederà una accurata preparazione e un processo pervasivo di accompagnamento)
5. servizi per la **configurazione** nella fase di avvio su tutte le strutture territoriali coinvolte, la **gestione operativa** e la **manutenzione** del sistema per la Gestione Digitale del Territorio per il periodo di 48 mesi successivi all'avvio (supervisione della pianificazione delle attività di sviluppo del SW, governo del progetto, tempi, costi e qualità)

## 4. Quadro economico dell'iniziativa

Si propone una stima di massima in relazione al valore complessivo delle attività citate e sulla base delle tariffe medie delle Gare messe a disposizione da Aria e Consip

Servizi Applicativi: 6milioni (punti 1, 2 e 3 del paragrafo 3)

Servizi Professionali: 2milioni (punto 4 del paragrafo 3)

Gestione operativa, manutenzione evolutiva e correttiva: 2milioni (punto 5 del paragrafo 3)

Alla presente stima dovranno essere aggiunte, valorizzate e pianificate le seguenti attività che Aria, già oggi, eroga per Regione Lombardia:

- Infrastruttura IT cloud dedicata alla Piattaforma Digitale Territoriale
- attivazione del supporto dell'Assistenza
- definizione delle Linee Guida a supporto della realizzazione delle integrazioni

## 5. Roadmap di attuazione

Si prevede di dar seguito alle attività di attuazione secondo il seguente macropiano, che potrà essere avviato a partire dall'assegnazione della fornitura:

- **2 mesi** – completamento della progettazione esecutiva del sistema e condivisione con Regione Lombardia;
- **3 mesi** - disponibilità delle funzionalità di base per l'accesso al sistema e dei principali servizi di integrazione con il Sistema Centrale Regionale
- **6 mesi** - disponibilità delle prime funzionalità del processo di valutazione, pianificazione e registrazione da rendere disponibili su tutto il territorio regionale;
- **9 mesi** - completamento dei servizi di integrazione del sistema di Gestione Digitale del Territorio con la piattaforma di esposizione in standard HL7 FHIR dei dati strutturati distribuiti nei sistemi informativi degli Enti; completamento delle integrazioni con il Sistema Centrale Regionale e con il FSE;

- **12 mesi** - disponibilità di funzionalità per la valutazione multidimensionale e per le valutazioni specialistiche, integrazione con i processi di telemedicina; estensione delle integrazioni HL7 FHIR con i sistemi presenti sul territorio;
- **a partire dall'avvio del sistema e per 48 mesi** – disponibilità di servizi di configurazione e avvio, gestione operativa e di manutenzione correttiva e evolutiva.

## 6. Strategia di procurement

Stante la necessità di dare rapido avvio all'iniziativa progettuale qui descritta, si riepilogano di seguito gli strumenti d'acquisto dei servizi valutati.

**Opzione 1: Strumenti contrattuali messi a disposizione da ARIA**

- **Servizi professionali**: Contratto ARIA (Gara 2/2019/LI - Procedura ristretta ai sensi dell'art. 61 del D.Lgs. n. 50/2016 per l'affidamento dei servizi di demand management, sviluppo, manutenzione per la realizzazione dei modelli di e-health della Regione Lombardia) – Lotto 1 (Welfare Regionale), attivo fino a giugno 2023.
- **Servizi applicativi**: Contratto ARIA (Gara 2/2019/LI - Procedura ristretta ai sensi dell'art. 61 del D.Lgs. n. 50/2016 per l'affidamento dei servizi di demand management, sviluppo, manutenzione per la realizzazione dei modelli di e-health della Regione Lombardia) – Lotto 4 (Servizi applicativi), attivo fino a giugno 2023.
- Successivamente, i servizi professionali, la gestione operativa e la manutenzione correttiva e evolutiva di quanto realizzato potranno essere assicurati accedendo alle convenzioni/contratti ARIA/convenzione Consip *pro tempore* disponibile.

**Opzione 2: Strumenti contrattuali messi a disposizione da Consip**

- **Servizi professionali**: Gara Consip (Gara a procedura aperta per la conclusione di un Accordo Quadro, ai sensi del d.lgs. 50/2016 e s.m.i., avente ad oggetto l'affidamento di servizi applicativi e l'affidamento di servizi di supporto in ambito «**sanita' digitale - sistemi informativi clinico assistenziali» per le pubbliche amministrazioni del SSN - ID Sigef 2202**) – Lotto 5 (Servizi di supporto per le Pubbliche Amministrazioni del SSN - Nord), attivo da gennaio 2022 con possibilità

di stipulare Contratti Esecutivi della durata di 48 mesi.

- **Servizi applicativi**: Gara indetta da Consip (Gara a procedura aperta per la conclusione di un Accordo Quadro, suddiviso in 7 lotti, con più operatori economici ai sensi dell'art. 54, comma 4 lett. c), d. lgs. n. 50/2016 e dell'art. 2, comma 225, Legge n. 191/2009, avente ad oggetto l'affidamento dei **servizi applicativi IT per le Pubbliche Amministrazioni — ID 1881**) – Lotto 4 (Contratti inferiori a 5 milioni– Area Nord). Il lotto 1 – Contratti superiori a 5 milioni di euro – Area Nord è concluso. È stata trasmessa una richiesta a Consip con la richiesta di aderire al lotto 4, ancora attivo, nonostante sia riservato a contratti di importo inferiore.
- Per attivare i servizi occorre indire un apposito Appalto Specifico per la stipula di un Contratto Esecutivo della durata massima di 48 mesi.
- Una possibile alternativa è il Lotto 2 dell'Accordo Quadro Consip **"Servizi Applicativi in ottica Cloud e PMO**" che dovrebbe essere attivato nel mese di gennaio 2022 (ipotesi da confermare).
- L'ulteriore iniziativa Accordo Quadro - **Servizi Applicativi e di supporto Sanità Digitale – Sistemi Applicativi clinico assistenziali** di Consip Spa non risulta disponibile in quanto in attesa del giudizio del procedimento di ricorso amministrativo. In questo caso occorre valutare la modalità di adesione attraverso rilancio competitivo o meno in base ai requisiti richiesti.

**Opzione 3: Mix di strumenti contrattuali messi a disposizione da ARIA e Consip**

- **Servizi professionali**: Gara Consip (Gara a procedura aperta per la conclusione di un Accordo Quadro, ai sensi del d.lgs. 50/2016 e s.m.i., avente ad oggetto l'affidamento di servizi applicativi e l'affidamento di servizi di supporto in ambito «**sanita' digitale - sistemi informativi clinico assistenziali» per le pubbliche amministrazioni del SSN - ID Sigef 2202**) – Lotto 5 (Servizi di supporto per le Pubbliche Amministrazioni del SSN - Nord), attivo da gennaio 2022 con possibilità di stipulare Contratti Esecutivi della durata di 48 mesi.

- **Servizi applicativi**: Contratto ARIA (Gara 2/2019/LI - Procedura ristretta ai sensi dell'art. 61 del D.Lgs. n. 50/2016 per l'affidamento dei servizi di demand

management, sviluppo, manutenzione per la realizzazione dei modelli di e-health della Regione Lombardia) – Lotto 4 (Servizi applicativi), attivo fino a giugno 2023. Successivamente, la gestione operativa e la manutenzione correttiva e evolutiva di quanto realizzato potranno essere assicurati accedendo alle convenzioni/contratti ARIA/convenzione Consip *pro tempore* disponibile.

Le Opzioni 1 e 3 non prevedono procedure di rilancio competitivo e, pertanto, consentono un immediato avvio delle attività progettuali. L'Opzione 2, qualora confermata percorribile da Consip, invece prevede, con riferimento ai Servizi Applicativi, necessariamente l'indizione di un apposito Appalto Specifico. Le tempistiche di norma necessarie al perfezionamento di tale iter portano a prefigurare, in questo caso, un avvio immediato per i Servizi Professionali – in analogia alle altre opzioni – ma un *elapsed* di circa sei mesi per l'attivazione dei Servizi Applicativi.

## 7. Caratteristiche specifiche del progetto attuativo

Come anticipato nel capitolo 3, le caratteristiche del sistema per la Gestione Digitale del Territorio dovranno recepire i vincoli e le interazioni derivanti dalla scelta di inserire questo componente nell'ecosistema digitale regionale che supporterà l'erogazione dei servizi sociosanitari sul territorio.

Il ruolo degli altri due componenti dell'ecosistema e le modalità di interazione funzionale con il sistema per la Gestione Digitale del Territorio sono sintetizzati di seguito:

- Piattaforma Regionale di Telemedicina: deve essere utilizzabile in maniera completamente integrata dai diversi contesti applicativi del sistema per la Gestione Digitale del Territorio, consentendo agli operatori di avvalersi delle diverse tipologie di processi e servizi di Telemedicina (es. televisite, telemonitoraggio, ecc.) per supportare e sostenere in modo strutturato e organizzato l'attuazione di interventi remoti di assistenza e cura verso i pazienti

- Nuova architettura per la raccolta e valorizzazione dei dati distribuiti: deve essere utilizzata dal Sistema per la Gestione Digitale del Territorio come unica infrastruttura di accesso ai dati distribuiti richiesti all'interno delle funzionalità del sistema, consentendo la condivisione e l'utilizzo in tempo reale dei dati prodotti presso i diversi servizi sociosanitari di ambito ospedaliero e territoriale.

Nei seguenti paragrafi verranno descritti i seguenti macro-elementi del progetto attuativo:

- analisi, progettazione e sviluppo delle **funzionalità applicative** specifiche necessarie a supportare in modalità completamente digitalizzata le attività di gestione delle Case della Comunità e delle Centrali Operative Territoriali *(paragrafo 4)*
- analisi, progettazione e sviluppo dei **servizi di cooperazione applicativa** necessari a garantire il funzionamento integrato con le altre componenti dell'ecosistema *(paragrafo 7.2)*
- implementazione delle **integrazioni con il Sistema Centrale Regionale** *(paragrafo 7.3)*
- conformità della proposta tecnica alle soluzioni tecnologiche e agli **standard architetturali** adottati nell'ecosistema, come richiesto dal contesto di forte integrazione del Sistema per la Gestione Digitale del Territorio nell'ecosistema digitale regionale *(paragrafo 7.4)*.

Relativamente ai restanti macro-elementi della proposta attuativa, che consistono nei **servizi professionali** per supportare l'attuazione del progetto e la diffusione della trasformazione digitale, nei **servizi per la configurazione** nella fase di avvio, nella **gestione operativa e** nella **manutenzione**, verranno adottate le modalità attuative, i modelli di erogazione e i livelli di servizio previsti dalla Convenzione Quadro tra Regione Lombardia e ARIA spa.

## 7.1. Funzionalità

Il sistema per la Gestione Digitale del Territorio verrà implementato in una **web application centralizzata multi-Ente**, in grado di offrire tutte le funzionalità

necessarie agli Enti nell'attuazione dei processi sociosanitari integrati ospedale-territorio e nel funzionamento operativo delle Case della Comunità e delle Centrali Operative Territoriali.

L'accesso degli utenti alla web application sarà gestito dal sistema regionale di **Autorizzazione**/**Autenticazione** IdPC di Regione Lombardia e la profilazione dei **diritti di utilizzo** delle specifiche funzionalità verrà regolato in maniera opportuna in base ai ruoli e ai privilegi di autorizzazione associati alle credenziali rilasciate a tutti gli utilizzatori, dal componente di provisioning del Sistema Centrale Regionale.

Le funzionalità del sistema per la Gestione Digitale del Territorio dovranno integrarsi con i servizi del Sistema Centrale Regionale nei contesti applicativi dove sia necessario accedere a **informazioni condivise a livello regionale**, come i dati identificativi dei pazienti contenuti nell'Anagrafe Regionale degli Assistiti (NAR), le codifiche degli Enti sociosanitari, i Nomenclatori delle prestazioni sociosanitarie e farmaceutiche, i dati codificati amministrativi (Comuni, Provincie, Regioni, Nazioni, ecc.).

L'interfaccia utente della web application deve rispettare gli **standard di design dei servizi digitali della Pubblica Amministrazione (PA) e le linee guida di Identità visiva di Regione Lombardia**, per favorire la massima usabilità, accessibilità ed ergonomia delle funzionalità.

Le funzionalità saranno realizzate in **maniera modulare**, attraverso una progettazione che identifichi gli ambiti applicativi omogenei a cui applicare soluzioni specializzate per tipologie di attività, come per esempio la pianificazione delle risorse, la gestione di workflow di compiti strutturati, la compilazione di questionari di valutazuione dei bisogni. I moduli dovranno essere strutturati in modo da ottimizzare i tempi di sviluppo e ottenere prestazioni elevate già sperimentate in domini applicativi in cui sono richieste funzionalità di analoga tipologia.

La modularità dello sviluppo applicativo e l'adozione delle Linee Guida di sviluppo previste per la PA abiliteranno la possibilità di pianificare sviluppi autonomi da parte di Regione Lombardia o di altri Enti pubblici che ne faranno richiesta.

Il seguente schema riassume i **moduli funzionali** richiesti:


- i seguenti moduli conterranno l'implementazione delle *integrazioni* con i servizi del Sistema Centrale Regionale:
    - **Autenticazione/Autorizzazione** per l'accesso al sistema e per la profilatura degli utenti all'utilizzo delle diverse funzionalità;
    - **NAR/Dati codificati** per l'identificazione dei pazienti e la classificazione dei dati strutturati;
    - **Gestione Relazioni Cittadino (CRM)** per l'invocazione dei servizi esposti dagli strumenti per la comunicazione integrata con il cittadino attraverso il Portale del Fascicolo Sanitario e per la ricezione dei messaggi inviati dal cittadino;
- i seguenti moduli conterranno le implementazioni a supporto dell'*operatività* delle strutture del Polo Territoriale (Case della Comunità/COT, ecc.):
    - **valutazione dei bisogni** per lo svolgimento delle analisi multidimensionali dei bisogni sanitari e socioassistenziali del paziente;
    - **gestione ordini** per attivare le richieste agli Enti erogatori e ai team di professionisti, assegnati alla Casa di Comunità, incaricati di eseguire interventi sul paziente

- **registro eventi** per monitorare l'attuazione di tali richieste, inclusa la ricezione degli esiti di tali interventi (es. rilevazione di parametri vitali o referti)
- **pianificazione risorse** per assegnare gli incarichi agli operatori, aggiornando i relativi calendari delle agende professionali personali
- **programmazione piani attività / calendar)** per collocare temporalmente tutti gli interventi necessari a prendere in carico il paziente e correlarle alla disponibilità delle risorse per l'attuazione dei piani
- **gestione workflow** per il coordinamento di tutte le attività pianificate, per l'implementazione dei controlli sulla sequenza delle operazioni svolte all'interno dei programmi di presa in carico del paziente;
- **configuratore dei moduli** per personalizzare i contenuti da rilevare durante le valutazioni dei bisogni e le checklist utilizzate nel monitoraggio dell'attuazione dei piani;
- **motore di regole** per implementare i criteri di classificazione dei bisogni a seguito della compilazione dei questionari di valutazione;

- i seguenti moduli conterranno le implementazioni di *strumenti trasversali* alle attività svolte dalle strutture del Polo Territoriale:
  - **strumenti automatizzati di supporto alle decisioni (DSS)** per assistere, al punto di cura, medici ed altri professionisti sanitari nel processo decisionale, fornendo, a titolo esemplificativo, analisi ed elaborazioni di dati relativi all'andamento storico del piano di presa in carico dei pazienti, con evidenza delle possibili correlazioni con informazioni cliniche e socioassistenziali specifiche dei pazienti.

    Il processo decisionale dovrà poter essere supportato anche da eventuali motori di regole esterni;
  - **strumenti di collaborazione** per garantire l'interazione digitalizzata tra gli operatori delle strutture coinvolte, attraverso le piattaforme di comunicazione interattiva multimediale, di condivisione della conoscenza e di messaggistica istantanea.

Di seguito vengono descritte le funzionalità al solo fine di delineare nel modo più preciso possibile il processo di assistenza territoriale: esse devono essere

considerate quali esigenze basilari che saranno oggetto di integrazioni in fase di progettazione esecutiva.

### 7.1.1. Funzionalità amministrative e di configurazione

Il sistema deve prevedere funzionalità generali di amministrazione e configurazione, che verranno svolte da operatori individuati specificatamente con un ruolo di Supervisore.

In tale insieme di funzionalità sono incluse:

- funzionalità di configurazione della rete territoriale per identificare le strutture da includere nel perimetro applicativo del sistema, attingendo ai dati centrali codificati che già identificano le relazioni organizzative delle strutture nell'ambito del territorio;
- funzionalità di configurazione delle relazioni tra i ruoli, le competenze e le funzionalità per singolo operatore o per profilo assegnato al Polo Territoriale;
- possibilità di caricare e/o configurare uno o più scale di valutazione preliminare e multidimensionale. Le scale di valutazione utilizzabili potranno essere sia scale standard definite da organismi nazionali o internazionali in ambito delle cure socio-sanitarie e assitenziali, di scale definite da modelli regionali, sia scale configurabili attraverso questionari definiti ad hoc e relativi algoritmi di calcolo della classe di complessità;
- funzionalità di gestione e configurazione di agende di disponibilità degli operatori: a titolo esemplificativo, ma non esaustivo, inserimento di slot di disponibilità dei professionisti della Casa di Comunità che compongono le équipe, configurazione di agende per la prenotazione di prestazioni specialistiche all'interno della Casa di Comunità. La visibilità e utilizzo di tali agende dipenderà dagli specifici ambiti funzionali e dovrà essere integrata con il planning di servizi e professionisti;
- configurazione degli step di processo e controllo (Workflow Management) e gestione di notifiche agli operatori e conferme di avvenuta esecuzione dell'attività con possibili *reminder* degli step successivi.

### 7.1.2. Funzionalità di collaborazione e comunicazione

Il sistema deve rendere disponibili funzionalità di collaborazione tra gli operatori delle Case di Comunità e delle COT consentendo:

- la gestione di calendari comuni e condivisi;
- la realizzazione di aree informative o bacheche elettroniche messe in comune per consultare documenti e linee guida di interesse comune;
- utilizzare soluzioni di comunicazione istantanea e notifiche (wiki, chat, sms).

### 7.1.3. Accettazione

L'applicativo deve gestire l'identificazione del cittadino per il quale è necessario prevedere il percorso di cura presso il distretto. Questa funzione deve permettere anche l'identificazione di un eventuale altro richiedente dei servizi (care giver, tutore) qualora fosse diverso dall'interessato.

In questa fase di accettazione si deve anche prevedere la compilazione della valutazione preliminare di bisogni o il recepimento della valutazione preliminare redatta da MMG-PLS o specialista ospedaliero.

L'accesso del cittadino alla Casa della Comunità e l'avvio del suo percorso di cura sul territorio devono essere caratterizzati da un numero identificativo che l'applicativo deve quindi generare in modo univoco.

Tale codice, rimarrà attivo per tutto il periodo di cura del cittadino. Il sistema dovrà generare un QR code contenente tale codice, associato ed eventuali altre informazioni, come per esempio il codice fiscale (C.F.) del cittadino e l'ambito territoriale, che dovrà essere reso disponibile al cittadino per facilitare il monitoraggio del suo percorso e gli accessi alla rete di servizi sociosanitari.

L'applicativo deve:

1. effettuare la ricerca anagrafica del cittadino sul Sistema Centrale dell'Anagrafica Regionale tramite inserimento/lettura del C.F.;

2. permettere la verifica di eventuale presa in carico del cittadino richiamando il servizio dedicato (Servizio di Base Gestione Presa in Carico GPC del SISS);
3. recuperare le informazioni utili quali numero di protocollo o identificativo del PAI;
4. consentire l'inserimento dei dati anagrafici del cittadino qualora la ricerca sul Sistema Centrale non produca risultati;
5. consentire l'inserimento dei dati di contatto del paziente (numero di cellulare, indirizzo mail);
6. registrare i dati del richiedente qualora il paziente interessato sia impossibilitato a presentarsi. Il richiedente va identificato tramite ricerca anagrafica sul Sistema Centrale o inserimento manuale;
7. eseguire la ricerca di segnalazioni relative alle dimissioni protette previste dai presidi del Polo Ospedaliero del distretto;
8. eseguire la ricerca di segnalazioni inserite dai cittadini sul portale Welfare, verificare la correttezza dei dati anagrafici interrogando l'Anagrafe Regionale e recepire eventuali dati mancanti;
9. eseguire la ricerca di segnalazioni di richieste di accesso ai servizi sociosanitari territoriali registrate da MMG-PLS o specialisti;
10. eseguire dei filtri sulle informazioni ricercate e ottenute dalle ricerche precedenti informazioni quali ad esempio C.F., provenienze segnalazione (portale Welfare/polo ospedaliero), ID della richiesta (numero di riferimento rilasciato da portale welfare/segnalazione di dimissione);
11. acquisire dall'Anagrafica Regionale o tramite inserimento manuale i riferimenti del MMG-PLS del paziente;
12. consentire l'inserimento del tipo di bisogno (semplice o complesso);
13. mostrare l'elenco di categorie (es. anziani, disabili, minori) e l'elenco di bisogni/servizio richiesti (es. centri diurni, assistenza domiciliare integrata, consultori) in relazione al tipo di bisogno;
14. raccogliere informazioni, per i casi di bisogno complesso, sulla modalità di esecuzione della successiva valutazione multidisciplinare: in presenza presso Casa della Comunità, al domicilio, con televisita, ecc.

15. consentire la raccolta delle informazioni di valutazione preliminare che può essere condotta presso la Casa della Comunità e inserita direttamente nel sistema o può recepire un modulo di valutazione preliminare precedentemente redatto da MMG-PLS o specialista; le informazioni riguardano le condizioni generali di salute del paziente, l'eventuale diagnosi clinica prevalente e secondaria, le condizioni di autonomia, autosufficienza e deambulazione, le capacità relazionali;
16. selezionare modelli predefiniti di valutazione preliminare dei bisogni;
17. calcolare tramite algoritmo definito il punteggio della valutazione preliminare (se tale punteggio è previsto);
18. consentire la registrazione delle informazioni anagrafiche e di contatto del caregiver;
19. attribuire un identificativo univoco alla richiesta registrata;
20. consentire l'upload di file per acquisire eventuali documenti presentati dal paziente/richiedente e utili ai fini degli step successivi del percorso;
21. prevedere la stampa di eventuali moduli da consegnare o di riepilogo per il cittadino.

### 7.1.4. Assegnazione équipe

La funzione di assegnazione dell'équipe deve permettere di identificare le figure professionali presenti nella Casa della Comunità che valutano il cittadino da un punto di vista clinico-sanitario e sociale, elaborano il progetto individuale e intervengono nel processo di cura del cittadino.

L'applicativo deve:

1. rendere disponibili le liste di accettazioni per le quali si è espresso un tipo di bisogno complesso e la necessità di eseguire la valutazione multidimensionale;
2. per ciascuna richiesta consentire di visualizzare e selezionare da un elenco le figure professionali che costituiscono l'équipe (MMG-PLS, assistente sociale, specialisti ecc.);

3. consentire di selezionare tra le figure professionali presenti nella Casa della Comunità il case manager da assegnare;
4. memorizzare l'informazione e renderla visibile nelle diverse maschere di riepilogo/moduli stampabili;
5. consentire il salvataggio dell'équipe costituita;
6. prevedere funzioni di modifica delle selezioni precedentemente effettuate;
7. una volta completata la composizione dell'équipe, abilitare una funzione di convocazione dell'équipe: visualizzare slot di disponibilità contemporanea di tutte le figure professionali da coinvolgere per la richiesta specifica tenendo conto della modalità di esecuzione indicata in fase di accettazione (in presenza presso Casa della Comunità, domicilio, televisita) e occupare gli slot per valutazione multidimensionale;
8. consentire di recuperare i dati di contatto del cittadino;
9. registrare in un campo note di contatto che il cittadino è stato chiamato per comunicare appuntamento per eseguire la valutazione multidimensionale, e il relativo esito del contatto (appuntamento confermato o rifiutato);
10. mostrare in modo evidente gli esiti del contatto verso il cittadino per gestire eventuali recall e ripianificazioni;
11. inviare una mail di riepilogo dell'appuntamento fissato al cittadino/caregiver.

### 7.1.5. Valutazione multidimensionale

La valutazione multidimensionale deve consentire alle figure dell'équipe di poter raccogliere in modo schematico informazioni riferite alle diverse dimensioni (clinica, funzionale, cognitiva, assistenziale) e la situazione socio-relazionale-ambientale della persona nella sua globalità per definire la necessità di servizi assistenziali e sviluppare un piano di assistenza e cura.

Le scale di valutazione da utilizzare devono includere quelle già adottate correntemente nei diversi ambiti socio-assistenziali: scala "home care" INTERRAI, scala SOSIA, scala SIDI, ecc.

Devono poter comunque essere utilizzate scale personalizzate e configurate all'interno del sistema, come descritto nel par. 7.1.1

L'applicativo deve:

1. mostrare alle figure dell'équipe la worklist quotidiana delle valutazioni multidimensionali da eseguire o da completare;
2. evidenziare in modo chiaro la modalità con cui la valutazione va eseguita ((in presenza presso Casa della Comunità, domicilio, televisita);
3. consentire la selezione della richiesta su cui lavorare e registrare il cambio di stato della segnalazione;
4. accedere alle informazioni della valutazione preliminare precedentemente inserita e ad eventuali moduli caricati nella fase di accettazione;
5. attivare la funzione di televisita nel caso sia questa la modalità di esecuzione della valutazione multidimensionale prevista;
6. selezionare uno o più scale di valutazione multidimensionale;
7. prevedere la possibilità di aggiungere indicazioni generali in campi note per completare eventuali informazioni di valutazione;
8. prevedere salvataggi parziali della valutazione multidimensionale per eventuali lavorazioni in tempi diversi;
9. gestire cambi di stato della segnalazione e prevedere viste di riepilogo delle segnalazioni filtrabili in base allo stato;
10. prevedere attivazione di teleconsulto nel caso questo si rendesse necessario tra le diverse figure professionali dell'équipe, o verso altri professionisti;
11. tenere traccia dei contatti avvenuti sia con il paziente, con il caregiver e tra l'équipe con campo note in cui riportare informazioni ritenute utili per gli step successivi;
12. generare un documento di valutazione multidimensionale, che può essere firmato digitalmente a cura del case manager e archiviato nel repository aziendale;

13. consentire la stampa della valutazione multidimensionale nel caso vada consegnata al cittadino;
14. salvare in forma strutturata le informazioni della valutazione e i metadati a supporto;
15. consentire di aggiornare una valutazione multidimensionale precedentemente salvata e non ancora conclusa;
16. annullare una valutazione multidimensionale precedentemente conclusa.

Il sistema deve prevedere anche l'utilizzo del modulo di supporto decisionale (DSS).

### 7.1.6. Gestione registrazione Consenso privacy al trattamento dati

L'applicativo deve disporre di funzioni che consentano di gestire modelli di consenso al trattamento dei dati del cittadino.

L'applicativo deve:

1. rendere disponibili i moduli di trattamento dei dati personali che si compilino automaticamente nelle sezioni di interesse con i dati inseriti a sistema nelle fasi di accettazione;
2. rendere possibile la stampa del modulo;
3. consentire upload di file firmati e scansionati;
4. consentire l'eventuale firma elettronica del modulo da parte del cittadino;
5. salvare il modulo sul repository aziendale;
6. consentire la consultazione dello stato di rilascio dei consensi da parte del cittadino.

### 7.1.7. Gestione del Progetto Individuale

L'applicativo deve gestire in questa funzionalità l'inserimento del piano delle attività in modo strutturato, mediante la compilazione di varie sezioni volte a definire il programma di cure in termini qualitativi, quantitativi e temporali.

L’applicativo deve prevedere l’inserimento di tutto il contenuto informativo necessario all’erogazione delle componenti del piano. Resta a discrezione dell’utente il grado di dettaglio da utilizzare in fase di compilazione. Pertanto, l’applicativo deve essere sufficientemente flessibile da consentire l’inserimento delle diverse prestazioni, farmaci o servizi con gradi di dettaglio differenti.

L’applicativo deve consentire di:

1. ricercare, a partire dalla lista di lavoro, eventuali valutazioni multidimensionali effettuate tramite l’utilizzo di differenti criteri di ricerca quali ad esempio l’anagrafica del cittadino, l’identificativo dell’episodio, l’identificativo della valutazione multidimensionale, il periodo temporale, l’identificativo del progetto di dimissione, ecc;
2. consultare l’esito della valutazione multidimensionale dell’équipe medica assegnata al paziente oppure il progetto di dimissione stilato dall’équipe di dimissione del polo ospedaliero ed in generale tutti i documenti esterni e tutte le altre informazioni sociosanitarie utili alla stesura del piano provenienti da attori esterni alla Casa della Comunità;
3. caricare modelli di piano (es. modelli di PDTA, modello di Piano Terapeutico Farmaceutico, modello di Piano terapeutico per Ossigenoterapia, ecc.) anche attraverso una fusione di uno o più modelli;
4. selezionare le prestazioni specialistiche/diagnostiche da inserire nel piano grazie all’integrazione con i cataloghi regionali delle prestazioni presenti nei Dati Codificati del Sistema Centrale Regionale;
5. indicare se tali prestazioni possono essere eseguite in telemedicina (es. televisita, teleassistenza, teleriabilitazione) oppure indicare specifiche prestazioni di telemedicina (es. telemonitoraggio);
6. inserire i farmaci necessari;
7. indicare le esigenze di protesica;
8. indicare le esigenze di ossigenoterapia;
9. indicare la necessità di interventi educazionali;

10. indicare la necessità di attivazione di servizi sociosanitari quali ad esempio: il ricovero presso strutture residenziali esterne alla Casa della Comunità (Ospedali di Comunità, RSA, Hospice, ecc..); i servizi di semiresidenzialità per anziani o disabili; i servizi di assistenza domiciliare (ADI, SAD, ecc.);
11. firmare digitalmente il documento che riporta il Piano delle attività redatto, archiviarlo nel repository aziendale ed eventualmente comunicarlo al Fascicolo Sanitario Elettronico, secondo gli scenari SISS di integrazione previsti;
12. generare e stampare un documento da consegnare al cittadino;
13. effettuare un teleconsulto con altro operatore (es. con membro équipe medica, medico dimettente, medico specialista, ecc.) al fine di completare la redazione del piano stesso;
14. tenere traccia delle interazioni con il cittadino;
15. aggiornare l'agenda delle figure professionali della Casa della Comunità che saranno coinvolte nell'attuazione del piano tenendo conto della modalità di esecuzione indicata (in presenza presso Casa della Comunità, domicilio, in telemedicina, ecc.);
16. prevedere salvataggi parziali per eventuali lavorazioni in tempi diversi;
17. indicare una data di fine validità del Piano;
18. richiamare il modulo di supporto decisionale (DSS).

Nel caso in cui la pianificazione richieda di richiamare informazioni presenti nei sistemi verticali regionali, come ad esempio, il sistema AssistantRL per gestire richieste di servizi di protesica, il sistema deve prevedere di richiamare tali applicativi tramite passaggio di contesto.

L'applicativo deve consentire le funzionalità di ricerca, modifica, aggiornamento e annullamento del Piano delle attività, notificando le modifiche.

### 7.1.8. Prescrizioni

In base alle prestazioni da erogare previste nel Progetto Individuale, l'applicativo deve:

1. aderire agli standard e normative vigenti in termini di generazione delle prescrizioni, sempre in linea con gli scenari di integrazione SISS;
2. identificare in maniera automatica le prestazioni e/o prescrizioni di farmaci presenti nel piano che necessitano di ricetta permettendo la stampa delle stesse;
3. in alternativa, richiamare eventuali moduli prescrittivi già esistenti (regionale o aziendali).

### 7.1.9. Prenotazione e attivazione di servizi

L'applicativo deve consentire di:

1. visualizzare la lista dei piani non ancora presi in carico secondo una scala di priorità o comunque filtrabile con una serie di criteri da definire;
2. effettuare la ricerca mirata di un piano (es. tramite diversi criteri di ricerca, quali ad esempio codice identificativo piano, dati paziente, ecc);
3. effettuare ricerche anagrafiche previa integrazione con l'Anagrafe Regionale;
4. una volta identificato il contesto, la prenotazione deve avvenire in maniera diversificata a seconda della tipologia:
    - **per prestazioni specialistiche:** il sistema deve garantire le esistenti funzionalità CUP standard ed in particolare deve consentire la ricerca delle disponibilità per l'erogazione di una o più prestazioni in tutte le strutture afferenti al Distretto di riferimento. Se non risultasse possibile individuare una soluzione nelle strutture del Distretto il sistema deve permettere l'integrazione con le agende di tutti i Distretti per ricercare una nuova disponibilità;
    - **per prestazioni di telemedicina,** il sistema deve garantire la comunicazione delle prestazioni da erogare alla piattaforma regionale previa integrazione con la stessa;
    - **per i servizi sociali e sociosanitari**: il sistema deve consentire di:

- consultare le disponibilità specifiche delle varie unità di offerta (es. ADI/SAD, Hospice, RSA, Ospedali di Comunità, Strutture Residenziali per disabili, Consultori, ecc.) mediante l'integrazione con il catalogo dell'offerta sociosanitaria del distretto o di altri distretti di riferimento;
- accedere ad eventuali piani tariffari per l'attivazione dei servizi;
- inserire la richiesta di attivazione anche per più strutture e inserire le conferme.

5. al termine della prenotazione, l'applicazione deve consentire la produzione di un documento riepilogativo delle prenotazioni e dei servizi attivati (compresi colloqui intermedi e finale di monitoraggio con il case manager/équipe) e consentire all'operatore di inviarlo al cittadino o altro attore interessato (tramite mail).

Le funzionalità di attivazione di servizi richiede l'implementazione del servizio di **Gestione del Catalogo di Offerta,** descritto successivamente nel par.7.1.11.

L'applicativo deve consentire le funzionalità di ricerca, modifica, aggiornamento e annullamento di prenotazioni, notificando le modifiche.

### 7.1.10. Riassegnazione della presa in carico territoriale

Nei casi di mobilità del cittadino (cambi di residenza, domicilio, trasferimenti temporanei, accessi alla Casa della Comunità di territori differenti) deve essere possibile trasferire la visibilità e i criteri di accesso del piano individuale e dei dati e dei documenti relativi al cittadino da un ambito competenza ad un altro (distretto/casa della comunità) consentendo la visualizzazione dei dati e dei documenti generati presso il/la precedente distretto/casa della comunità.

### 7.1.11. Servizio di gestione catalogo di unità di offerta

Il sistema deve gestire il **catalogo di Unità di Offerta** per tipologia di intervento necessario per realizzare la programmazione prevista per il cittadino.

Il catalogo di Unità di Offerta viene alimentato con informazioni sul livello di occupazione della risorsa delle unità di offerta (es. ADI, Hospice, RSA, Ospedali di Comunità, ecc). Queste informazioni sono acquisite accedendo al componente Dati Distribuiti che espone le informazioni nel formato di risorse HL7 FHIR, come descritto nel seguente par.7.2 .

Il servizio di gestione del catalogo di unità di offerta deve prevedere le seguenti operazioni dettagliate nel seguito:

### a. Elenco delle informazioni del catalogo generale di unità di offerta

Il sistema deve richiedere e disporre dell'elenco complessivo delle strutture per territorio. Per ciascuna struttura si prevedono presenti i seguenti dati:

- Codice e descrizione della struttura
- Territorio (ATS, ASST, distretto) di afferenza, o per cui è accreditata
- Tipologia di struttura (RSA, ADI, CDD…)
- Indirizzo

| **Ambito** | **Descrizione** | **Vista Dati codificati** | **Tipologia struttura Dati Codificati** |
|---|---|---|---|
| Sanitario | Presidio Ospedaliero | V_LR_LIVELLO_2 | SAN |
| Sociosanitario | Assistenza domiciliare integrata (ADI) | V_LR_LIVELLO_2 | SAN |
| Sociosanitario | Centri Diurni per persone con disabilità (CDD)) | V_LR_LIVELLO_2 | CDD |
| Sociosanitario | Centri Diurni Integrati (CDI) | V_LR_LIVELLO_2 | CDI |
| Sociosanitario | Residenza Sanitaria per persone Disabili (RSD) | V_LR_LIVELLO_2 | RSD |
| Sociosanitario | Comunità Sociosanitarie per disabili (CSS) | V_LR_LIVELLO_2 | CSS |
| Sociosanitario | Residenza Sanitaria Assistenziale (RSA) | V_LR_LIVELLO_2 | RSA |
| Sociosanitario | Hospice | V_LR_LIVELLO_2 | SAN e TIPO STRUTTURA=RESIDENZIALE |
| Sociosanitario | Consultori Familiari | V_LR_LIVELLO_2 | SAN e TIPO STRUTTURA=ALTRO TIPO DI STRUTTURA TERRITORIALE |
| Sociosanitario | Servizi dipendenze (SerT) | V_LR_LIVELLO_2 | SAN e TIPO STRUTTURA=ALTRO TIPO DI STRUTTURA TERRITORIALE |
| Sociosanitario | Strutture di riabilitazione e cure intermedie (RIA/INT) | V_LR_LIVELLO_2 | SAN e TIPO STRUTTURA=ALTRO TIPO DI STRUTTURA TERRITORIALE |

| | | | |
|---|---|---|---|
| Sociosanitario | Strutture cure palliative (UOCP) | V_LR_LIVELLO_2 | SAN e TIPO STRUTTURA=ALTRO TIPO DI STRUTTURA TERRITORIALE |
| Sociosanitario | Cure domiciliari per i malati terminali (UCP-DOM) nata dalla riclassificazione dell'attività ADI | V_LR_LIVELLO_2 | SAN e TIPO STRUTTURA=ALTRO TIPO DI STRUTTURA TERRITORIALE |

**b. Servizio di interrogazione e acquisizione del livello di occupazione e calcolo delle disponibilità secondo driver specifici per tipologia di unità di offerta.**

Per tipologia di servizio e di struttura per cui l'operatore di COT deve avviare la richiesta, il sistema invoca un servizio per richiedere il livello di occupazione delle risorse dell'unità di offerta.

Questa richiesta è indirizzata agli Enti erogatori dei servizi. La risposta consiste nell'informazione del numero di risorse occupate, raggruppate per la tipologia di struttura presente nel territorio e messe a disposizione dal sistema di dati distribuiti (vedi par. 7.2).

Il livello di occupazione è determinato secondo differenti indicatori, diversi per tipologia di unità di offerta:

- Strutture residenziali anziani RSA: posto letto per tipologia di paziente (a titolo esempio: normale o Alzheimer)
- Strutture semiresidenziali (CDD; CDI; CSS): posto letto, frequenza e fascia oraria
- ADI: disponibilità di un "pacchetti di servizi" su cui effettuare un ordine
- Hospice: posto letto
- Presa in Carico: numero arruolati per Gestore
- Strutture residenziali Disabili (SIDI): posto letto per classe SIDI
- Unità di Offerta Terapia del Dolore/Cure Palliative Domiciliari: posto letto per tipologia di paziente
- Consultori: frequenza e fascia oraria
- UOP Psichiatria: posto letto per tipologia di paziente
- Servizi Dipendenze SERT: frequenza e fascia oraria

A titolo di esempio le regole possono essere riepilogate nella seguente tabella:

| Tipo Unità di Unità di Offerta | Struttura | Driver di occupazione |
|---|---|---|
| Residenziale | Residenza Sanitaria Assistenziale (RSA) … | Posto letto accreditato a contratto per tipologia paziente (es: posto letto normale, posto letto per Alzheimer) |
| Semiresidenziale | Centri Diurni | Posto letto, frequenza e fascia oraria |
| ADI | Assistenza domiciliare integrata (ADI) | Numero di ordini (richieste) (Tipologia order Entry) |

### c. Raccolta delle disponibilità massime totali per unità di offerta

Data la tipologia di unità di offerta che l'operatore di COT ricerca, il sistema mostra per tutte le strutture presenti sul territorio il livello di occupazione, rappresentato da indicatori quantitativi aggregati, come per esempio livello basso-medio-alto.

Questi indicatori devono essere calcolati confrontandoli con l'informazione relativa al numero massimo di risorse a disposizione, per confrontarle rispetto alle risorse occupate.

Il sistema richiede al registro di accreditamento delle strutture sociosanitarie (AFAM) l'informazione sul numero massimo di risorse gestite per struttura e servizi dichiarati per l'accreditamento della struttura.

Laddove tutte le strutture del territorio della COT risultassero con livelli di occupazione elevati, l'operatore opzionalmente potrà chiedere l'interrogazione di risorse di altri territori.

### d. Funzionalità per la gestione di criteri a supporto della selezione dell'unità di offerta

L'operatore di COT deve poter ricercare le strutture rispondenti al bisogno del cittadino anche sulla base di servizi offerti.

Per la ricerca e selezione di strutture residenziali a compartecipazione della spesa da parte del cittadino è fondamentale la disponibilità dell'informazione relativa alla retta: il sistema fornirà all'operatore tale informazione.

In tale elenco, per le risorse relative a strutture residenziali (es. RSA) deve essere presente l'informazione della retta dichiarata dalla struttura.

**e. Funzionalità per la selezione dell'unità di offerta e funzionalità di monitoraggio delle conferme e gestione dei rifiuti e ri-selezione di nuova struttura con disponibilità.**

Individuata la struttura sulla base della disponibilità e dei servizi erogati, l'operatore di COT deve poter confermare la richiesta di occupazione della risorsa.

La richiesta deve essere acquisita dal sistema e trasferita alla struttura.

L'operatore di COT deve avere una funzionalità che permetta il monitoraggio delle richieste inoltrate alle strutture con lo stato di avanzamento della richiesta (es: inviata, in lavorazione, confermata, rifiutata, cancellata).

I sistemi verticali di gestione delle strutture devono poter invocare il sistema attraverso le interfacce HL7 FHIR per controllare le richieste pervenute, eventualmente notificate anche tramite mail ad una casella definita, e gestire la conferma di acquisizione della richiesta o il rifiuto.

### 7.1.12. Monitoraggio dell'attuazione del Progetto Individuale

L'applicativo deve fornire una serie di strumenti per il monitoraggio dell'attuazione del Progetto Individuale tramite un motore di Workflow Management che gestisce e traccia gli stati di avanzamento del progetto sulla base degli interventi dei diversi attori coinvolti nella esecuzione del piano.

In particolare, l'applicativo deve:

1. consentire una visione "unitaria" e di monitoraggio del Piano e dello stato di esecuzione:
    - delle prestazioni sanitarie sociali e sociosanitarie;
    - delle prestazioni erogate in Telemedicina

    in un unico strumento in grado di fornire al Case Manager in ogni momento uno "snapshot" della situazione dell'assistito nel suo complesso;

2. rappresentare in modo grafico ed intuitivo l'evoluzione del percorso con la possibilità di zoom su giorno/settimana/mese anno e/o su un periodo specifico;
3. avere una visione immediata dello stato di esecuzione delle prestazioni e consultazione degli esiti clinici (anche di telemonitoraggio)
4. consentire la consultazione delle rilevazioni contenute nel diario degli interventi prodotto dagli erogatori;
5. interagire con il MMG-PLS/équipe/case manager per eventuali necessità di modificare la programmazione a fronte degli esiti clinici;
6. mettere a disposizione una dashboard ("Checklist") per il monitoraggio delle attività in scadenza e/o scadute, filtrabile per tipologia di attività, équipe e periodo di interesse; le checklist di valutazione dell'esecuzione del progetto dovranno essere configurabili e modificabili tramite apposite funzioni di gestione.
7. visualizzare in modo chiaro tutte le informazioni utili relative all'assistito (contatti, équipe, problematiche presenti ecc.).

Ogni azione (es. Prescrizione, prenotazione, esecuzione, refertazione) finalizzata all'erogazione di una prestazione deve essere assegnata, in fase di creazione (arruolamento) e/o aggiornamento del piano, ad un "esecutore", che può essere:

- un professionista (MMG-PLS, Infermiere, Specialista, Assistente Sociale, ecc.)
- una équipe specialistica
- il caregiver
- il paziente stesso (attività relative allo stile di vita come passeggiate, palestra ecc. o consumo di medicinali).

Ogni azione deve essere rendicontata nei tempi previsti dal Piano dal soggetto esecutore.

L'applicativo deve:

1. definire e configurare workflow di processo;
2. mettere a disposizione strumenti di assegnazione ai componenti del Team Multidisciplinare (équipe) delle azioni necessarie all'erogazione della prestazione (es. Prescrizione (MMG-PLS), prenotazione (COT), esecuzione (Professionista), refertazione (Professionista));
3. mettere a disposizione strumenti di alert per erogatori, pazienti e caregiver;

4. dare la possibilità di dare evidenza dell'esecuzione dell'azione assegnata su piattaforma web e APP;
5. dare la possibilità di esporre API verso erogatori esterni che utilizzano sistemi propri.

### 7.1.13. Diario multidisciplinare

L'applicativo deve fornire uno strumento di condivisione delle informazioni relative alla gestione del paziente.

Tale strumento deve consentire uno scambio strutturato e in sicurezza delle informazioni e delle attività svolte dagli attori coinvolti nella esecuzione del Progetto Individuale, come per esempio, dagli operatori della Centrale Operativa Territoriale e dai professionisti.

A titolo di esempio, il diario deve riportare il riepilogo di un colloquio con il MMG-PLS, annotazioni di un intervento di assistenza domiciliare ed altri eventi svolti nel corso del processo.

### 7.1.14. Rendicontazione

Tutti i dati raccolti dal sistema di gestione del territorio nelle diverse fasi del processo sanitario e sociosanitario devono essere resi disponibili nelle diverse forme richieste anche ai fini della rendicontazione.

### 7.1.15. Telemedicina

Attraverso l'applicativo deve essere possibile interagire con la piattaforma di telemedicina.

L'applicativo deve poter invocare strumenti di:

- Televisita
- Teleconsulto
- Telemonitoraggio
- Teleassistenza

Questi strumenti saranno abilitati attraverso la piattaforma di telemedicina integrata all'applicativo.

Ognuno di questi servizi deve consentire di restituire all'applicativo le informazioni relative all'erogazione, quali ad esempio, a titolo non esaustivo:

- Televisita: referto della televisita
- Teleconsulto: referto condiviso o relazione contributiva del medico a cui viene richiesto il consulto
- Telemonitoraggio: dati di sintesi del monitoraggio con eventuale evidenza di allarmi/anomalie e valutazione finale
- Teleassistenza: dati di sintesi della seduta di riabilitazione con eventuale evidenza di allarmi/anomalie.

## 7.2. Servizi di cooperazione applicativa

Le funzionalità del sistema per la Gestione Digitale del Territorio descritte nei paragrafi precedenti richiedono lo scambio di informazioni e di contesti applicativi con le altre componenti dell'ecosistema attraverso interfacce applicative che consentono l'utilizzo integrato delle funzioni svolte dai diversi componenti.

Queste interfacce devono essere implementate attraverso servizi di cooperazione progettati in funzione delle specifiche modalità di interazione con i due componenti descritti nell'introduzione del capitolo 7.

Le modalità di funzionamento dei servizi si differenziano come descritto nel seguito:

<u>Telemedicina:</u>

il presupposto per l'interazione con questo componente è che la soluzione di Telemedicina venga implementata come sistema unico regionale multi-Ente, all'interno del quale verranno esposti gli specifici microservizi dedicati alle funzionalità: televisita e telerefertazione, telemonitoraggio, teleconsulto, telemonitoraggio, teleassistenza.

Questi microservizi potranno essere richiamati dall'interno del contesto applicativo del sistema Gestione Digitale del Territorio, per esempio nella funzionalità Accettazione per richiedere una televisita o nella funzionalità di Prenotazione e attivazione di servizi per avviare un telemonitoraggio.

La piattaforma di Telemedicina potrà inviare i dati strutturati che rappresentano gli esiti conseguenti allo svolgimento di queste funzionalità invocando un

microservizio dedicato alla ricezione, esposto dal Sistema per la Gestione Digitale del Territorio.

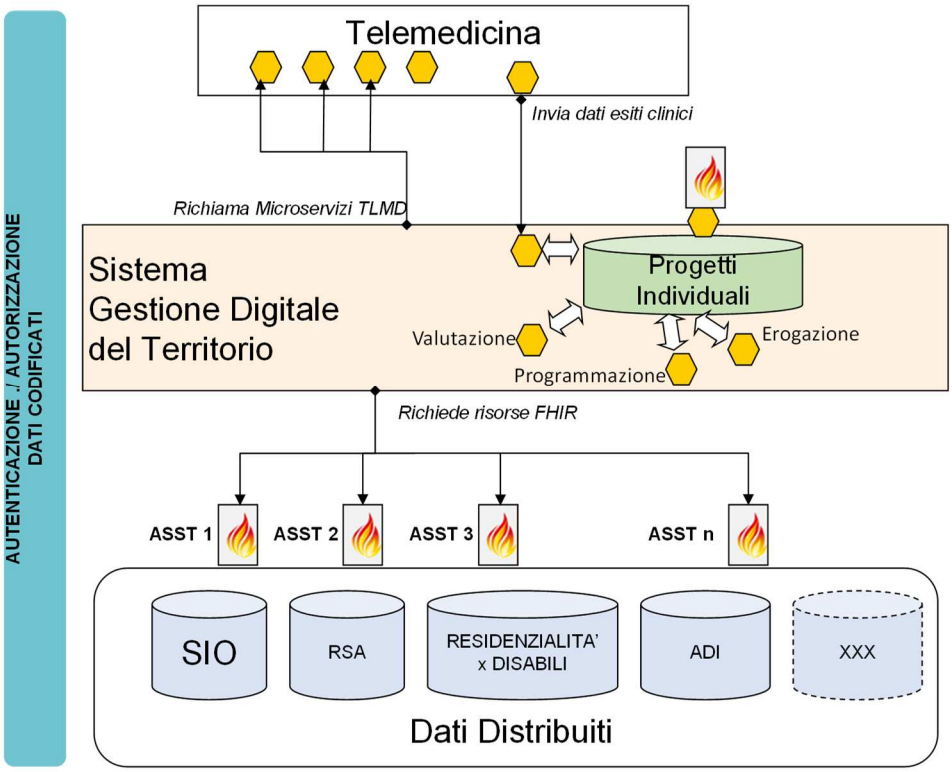
La modalità di interazione con il componente Telemedicina richiede l'implementazione quindi di DUE tipi di Servizi nel sistema Gestione Digitale del Territorio: 1) interfacce applicative per invocare le API (Application Programming Interface) di Telemedicina dagli opportuni contesti applicativi; 2) esposizione di API richiamabili dal sistema di Telemedicina per la ricezione degli esiti.

Dati Distribuiti:

questo componente deve essere implementato come un'infrastruttura regionale con opportuni punti di accesso ai dati distribuiti esposti attraverso un'interfaccia standard HL7 FHIR per ognuna delle ASST. L'accesso a questi dati da una funzionalità del Sistema per la Gestione Digitale del Territorio deve avvenire tramite una richiesta di una Risorsa FHIR che rappresenta una entità informativa. In questo modo il sistema potrà acquisire informazioni come, ad esempio: elenco di dimissioni programmate memorizzate nel Sistema Informativo Ospedaliero di una ASST, elenco dell'occupazione delle risorse di un Ente socioassistenziale, esito di attività svolte per l'assistenza domiciliare e memorizzate nel sistema verticale, PAI generati dagli enti erogatori, ecc..

La modalità di interazione con il componente Dati Distribuiti richiede l'implementazione quindi di servizi costituiti da interfacce applicative per invocare le API RESTful modellate secondo lo standard HL7 FHIR, esposte dalle istanze Gateway FHIR di ciascuna ASST.

Lo schema riassume il disegno dei Servizi e il loro ruolo per la comunicazione tra i diversi componenti.




Il sistema per la Gestione Digitale del Territorio include i microservizi che implementano le macrofunzionalità di Valutazione, Programmazione e Erogazione dei Progetti Individuali, come descritto nei paragrafi precedenti. Oltre a ciò, il sistema deve esporre microserviservizi di consultazione dei dati generati nel corso dei processi supportati dalle funzionalità del sistema e raccolti nei Progetti Individuali. Questi dati sono modellati come risorse HL7 FHIR v.4. Le risorse FHIR potranno essere consultate dalle applicazioni di ASST ed enti del territorio secondo opportuni criteri di autorizzazione.

L'interazione con il *COMPONENTE TELEMEDICINA* presuppone che esso esponga le API (Application Programming Interface) per ogni funzione, le cui specifiche verranno condivise con il sistema regionale di Telemedicina. Pur non essendo ancora stata individuata la specifica soluzione di mercato, la piattaforma che verrà implementata avrà alcune caratteristiche fondamentali, comuni alle più moderne proposte tecnologiche di Telemedicina.

In particolare, si presuppone che il sistema regionale di Telemedicina sia basato su un'architettura modulare, all'interno della quale saranno presenti i Microservizi dedicati alle funzioni di televisita e telerefertazione, telemonitoraggio, teleconsulto, telemonitoraggio, teleassistenza. Le API che richiamano i microservizi devono essere esposte da un componente API Manager della piattaforma di Telemedicina.

Nel progetto attuativo si prevede l'analisi dettagliata del contesto applicativo del Sistema Gestione Digitale del Territorio nel quale l'operatore possa attivare le funzioni di Telemedicina e l'implementazione delle interfacce per **richiamare le API esposte dai moduli di Telemedicina**. Il sistema deve poter utilizzare i parametri di invocazione necessari a eseguire in maniera coerente le funzionalità di telemedicina, come per esempio: Anagrafica Paziente, Identificativo dell'Operatore medico/infermieristico che svolge la funzione di telemedicina, Data di esecuzione dell'Evento di telemedicina, Identificativo e caratteristiche tecniche di tale Evento.
La piattaforma di Telemedicina condividerà i servizi infrastrutturali di Identity/Access Management per l'autenticazione e l'autorizzazione e di Master Data per la gestione di dati codificati.
L'interazione con la piattaforma di Telemedicina richiede inoltre di **esporre API da parte del Sistema Gestione Digitale del Territorio.** Nel progetto attuativo si prevede quindi la progettazione e l'implementazione di un microservizio di memorizzazione di dati strutturati nella base dati centralizzata del sistema. L'API esposta da tale microservizio deve essere richiamata identificando in maniera coerente i parametri che associano gli esiti delle funzionalità di telemedicina al contesto dei Piani Individuali a cui si riferiscono, come per esempio: Paziente, Identificativo univoco dell'Evento, Dati strutturati di Esito.

L'interazione con il *COMPONENTE DATI DISTRIBUITI* si basa su un'infrastruttura che renderà disponibile in tempo reale i dati prodotti presso i diversi servizi sociosanitari di ambito ospedaliero e territoriale. Questa infrastruttura avrà le seguenti caratteristiche:

- esiste un'identificazione univoca dell'**attore responsabile** della generazione, della validazione dei dati e della memorizzazione in uno stato di persistenza (database), corrispondente all'Ente responsabile dei dati clinici,

socioassistenziali e amministrativi che sono condivisi da diversi utilizzatori coinvolti nei percorsi di assistenza e cura del cittadino;

- viene esposta per tutte le entità una rappresentazione standardizzata dei dati in un'**unica interfaccia di consultazione** strutturata, accessibile da tutti i componenti dell'ecosistema, evitando la duplicazione delle informazioni su più basi dati;
- viene garantito l'**accesso diretto e controllato** ai dati da parte degli utilizzatori autorizzati attraverso l'esposizione di un'univoca locazione (*endpoint*) delle risorse che rappresentano i dati;
- sono disponibili meccanismi per il **consolidamento dei dati** a livello dell'intera Regione Lombardia, per utilizzi diversificati rispetto al processo operativo di assistenza e cura.

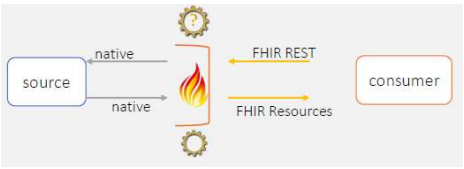
L'integrazione del sistema con questa infrastruttura di dati distribuiti deve basarsi sulla **modellazione definita nello standard FHIR** v.4 di HL7 di tutte le entità informative scambiate nel processo di assistenza e cura nei poli Ospedaliero e Territoriale dell'ASST e memorizzate sulle basi dati distribuite nei sistemi informativi degli Enti coinvolti. L'implementazione del modello HL7 FHIR non comporta necessariamente la modifica della struttura dei dati nei database dove le informazioni stesse vengono generate, memorizzate e aggiornate dalle funzionalità dei diversi ambiti applicativi (es. da moduli interni del SIO, da sistemi informativi a supporto delle RSA, ecc.).

Ogni entità informativa che è necessario condividere in tutto l'ecosistema corrisponde ad una **"Risorsa FHIR"** accessibile tramite il modello di consultazione adottato da HL7 FHIR.

L'accesso alle Risorse FHIR deve avvenire attraverso API RESTful, cioè tramite interfacce che definiscono i metodi di lettura, scrittura, aggiornamento, ricerca, ecc. delle risorse stesse. Queste API devono essere implementate sulle istanze di **"Server FHIR"**, ciascuno dei quali costituirà quindi l'univoca locazione (*endpoint*) esposta per l'accesso al dato certificato che rappresenta una certa entità all'interno dell'ecosistema.

I “Server FHIR” che devono essere implementati nell’infrastruttura dei dati distribuiti agiranno da traduttori (*gateway*) nei confronti del “Content Consumer”. Il gateway accederà ai dati necessari alla rappresentazione FHIR attraverso le modalità native del sistema sorgente.

Il seguente schema rappresenta la modalità *gateway* che deve essere implementata sui server FHIR:




Per l’implementazione dei “server FHIR” devono essere realizzati opportuni servizi nella **Piattaforma di Integrazione NPRI**, utilizzando le istanze dedicate a ciascuna ASST, alle ATS e l’istanza del Dominio Centrale.

Questa opportunità consente di superare il vincolo che all’interno di ogni Ente esistano soluzioni applicative eterogenee dal punto di vista della strutturazione dei dati clinici-assistenziali. La NPRI implementerà un **componente Gateway FHIR** in grado di mappare le informazioni generate dagli specifici applicativi degli Enti con il modello logico FHIR.

L’architettura dei dati sarà costituita dai seguenti elementi:

- **un server NPRI con gateway FHIR per ogni ASST** per esporre le “Risorse di tipo clinico, socioassistenziale e amministrativo”, come ad esempio: episodio di ricovero con dimissione programmata, esito di accertamento diagnostico, disponibilità di posti letto di una RSA, nota di diario ADI, PAI redatto da una struttura socioassistenziale, ecc.;
- **un Repository documentale per ogni ASST** per memorizzare i documenti clinici-assistenziali generati dalle funzionalità di Valutazione/Programmazione/monitoraggio (es. PAI, scheda di valutazione multidimensionale, ecc.);

- **un server NPRI con gateway FHIR di Dominio** per esporre le “Risorse di tipo trasversale” (es. informazioni demografiche di un paziente, codifica di una Struttura, anagrafica e ruolo di un medico, ecc.);
- **servizi FSE** per la consultazione dei referti e dei dati auto contribuiti dal Cittadino, collocati nel Taccuino personale.

## 7.3. Integrazioni con il Sistema Centrale Regionale

Il sistema per la Gestione Digitale del Territorio si inserirà all’interno dell’infrastruttura a supporto del Sistema Centrale Regionale e deve di conseguenza implementare le integrazioni previste per i seguenti scenari indicati di seguito e le integrazioni con i Servizi al Cittadino.

Gli scenari sono quelli di seguito riportati, don il relativo riferimento alla documentazione di progetto presente sul sito “Documentazione SISS”:

- identificazione Cittadino e allineamento anagrafiche (cfr. DC-SCEN-ICCE#01)
- Gestione del Documento Clinico Elettronico presso gli Enti Erogatori **(**DC-SCEN-REF#01);
- gestione prescrizioni (DC-SCEN-PRSC#01);
- gestione Prenotazioni per Enti Erogatori (DC-SCEN-PRE#101);
- integrazione tra Gestione Presa in Carico GPC e SISS (DC-SCEN-GPC#01);
- gestione dell’Accoglienza - Comunicazione degli eventi sanitari ospedalieri al FSE (DC-SCEN-ACCO#01);

Le integrazioni da implementare riguardano in particolare le funzioni di

- funzione Accettazione descritta nel par. 7.2.2 per l’identificazione del cittadino nella anagrafe regionale NAR;
- funzione di Gestione del Progetto Individuale descritta nel par. 7.2.6 per la gestione dei documenti prodotti nella formulazione del piano e per le funzioni di prescrizione elettronica;
- funzione di Prenotazione e Attivazione Servizi o Individuale descritta nel par. 7.2.8 per la gestione delle prenotazioni.

Relativamente all'integrazione con i Servizi al Cittadino, devono essere realizzati gli opportuni microservizi per abilitare il cittadino a eseguire servizi online. A titolo esemplificativo questi servizi sono: l'invio di richieste al proprio MMG-PLS o al Caregiver , la prenotazione dell'accesso al Punto Unico di Accesso (PUA), la visualizzazione di eventi programmati, la visualizzazione dei propri piani e il relativo stato di avanzamento, la ricezione di notifiche di avanzamento delle proprie pratiche e del progetto.

Queste funzioni sono finalizzate a favorire un maggior empowerment del cittadino nelle interazioni con strutture, servizi ed operatori del Sistema Territoriale.

Il Sistema per la Gestione Digitale del Territorio deve pertanto esporre servizi per l'integrazione con il Sito del Fascicolo Sanitario e dei Servizi Digitali, con l'App Fascicolo Sanitario e prevedere la comunicazione di notifiche al sistema di gestione centralizzata delle notifiche regionale.

Tale sistema di gestione notifiche già prevede di identificare il consenso raccolto, il canale da utilizzare e gestisce anche il contatto validato, rendendo inoltre disponibile una dashboard di controllo delle proprie notifiche, accessibile dal sito Fascicolo Sanitario in cui in ogni momento l'interessato può cambiare le proprie preferenze.

## 7.4. Architettura tecnologica

Il progetto attuativo del sistema per la Gestione Digitale del Territorio deve essere conforme alle soluzioni tecniche e agli standard adottati nell'ecosistema:

- **Architettura Microservizi**
  - Al fine di soddisfare gli obiettivi di business, correnti e futuri, il sistema per la Gestione Digitale del territorio deve adottare una architettura a microservizi (service-based architecture). Pertanto, il Sistema per la Gestione Digitale del Territorio deve essere organizzato come un insieme di microservizi.
  - L'architettura funzionale del sistema deve essere modulare: ogni modulo deve essere costituito da un insieme omogeneo e coerente di microservizi.

- La comunicazione tra microservizi e tra *client* e *server* deve essere realizzata con protocolli di comunicazione sicuri (es. https).

- **API Manager**
  - Il sistema deve adottare un API Manager per monitorare, ottimizzare e rendere sicuro l'utilizzo delle API tramite il controllo degli accessi, l'applicazione delle policy di sicurezza, il routing, il caching, gli strumenti di analisi e monitoraggio.
  - Poiché i moduli del Sistema per la Gestione Digitale del Territorio dovranno interagire come singole funzionalità separate e indipendenti tra loro, ma fortemente integrate con gli altri componenti presenti nell'ecosistema, è necessario che il sistema per la Gestione del Territorio esponga tutti i servizi attraverso un API Manager.
  - L'applicativo deve connettersi anche all'API Manager del Sistema Centrale Regionale al fine di utilizzarne i servizi. Per tale connessione, i servizi che invocheranno le interfacce esposte dall'API Manager dovranno sempre esplicitare il Profilo utente che vuole effettuare l'accesso in modo da ottenere l'Authorization Code (code) per accedere ai servizi dell'API Manager.

- **Sistema autenticazione/autorizzazione al Sistema Centrale Regionale**
  - Il Sistema per la Gestione Digitale del Territorio per le funzioni di autenticazione / autorizzazione deve utilizzare i servizi messi a disposizione del Sistema Centrale Regionale.
  - L'accesso all'applicazione deve avvenire utilizzando il sistema di autenticazione IdPC di Regione Lombardia che applicherà tutti i controlli di accesso necessari
  - I privilegi di autorizzazione ad utilizzare le differenti funzionalità sono basati sul sistema di provisioning del Sistema Centrale Regionale che definisce i ruoli degli utenti e la loro associazione alle strutture organizzative

- **Cloud Nativo**
  - Il sistema per la Gestione Digitare del Territorio deve essere Cloud Native ovvero concepito, progettato e sviluppato appositamente per poter operare in ambiente cloud.
  - Come tecnologia di orchestrazione dei container deve essere adottata OpenShift.
  - L'applicazione deve essere conforme all'utilizzo su un cloud di tipo Platform-as-a-Service (Paas).

- **Garanzia utilizzo codice sorgente**
  - Il codice sorgente deve essere disponibile su un repository (es. sourceSafe) che ne gestisca anche il versioning.
  - Nel codice sorgente devono essere presenti commenti che spieghino i blocchi di codice a cui si riferiscono.
  - Deve essere presente una documentazione tecnica.
  - Deve essere presente una documentazione funzionale.
  - Il processo di test e rilascio di ogni versione dell'applicativo deve seguire le best practices di tracciamento e automazione del ciclo di vita del software.

- **Certificazione:**
  - Il Sistema per la Gestione Digitale del Territorio deve essere predisposto per essere sottoposto ai percorsi previsti dalla normativa vigente per acquisire la certificazione come dispositivo medico.

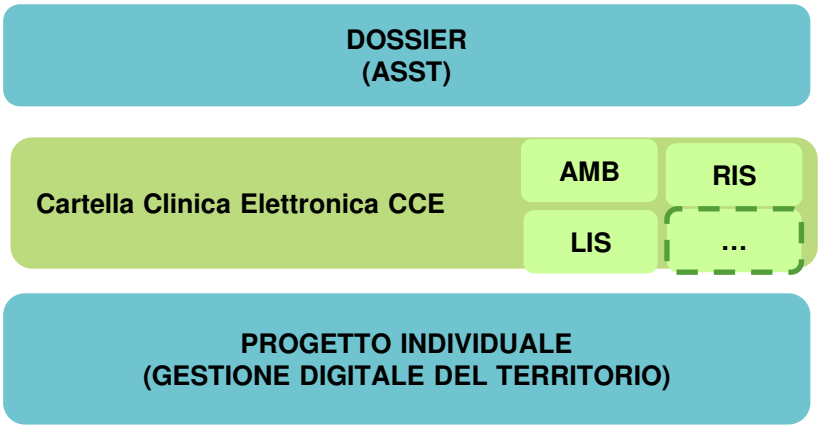
# 8. Privacy e Sicurezza

## 8.1. Livelli di condivisione dei dati

Si ritiene opportuno premettere alle considerazioni relative alla privacy e alla sicurezza un richiamo ai livelli di condivisione dei dati, che sono peculiari del processo implementato nell'ecosistema di gestione delle cure territoriali, caratterizzato da una forte eterogeneità e distribuzione dei sistemi informativi utilizzati.

Si possono identificare almeno **tre livelli** che corrispondono a diverse finalità di raccolta e consultazione dei dati sanitari di un cittadino da parte degli operatori coinvolti nei percorsi di assistenza e cura forniti al cittadino stesso.

Il seguente schema rappresenta questi livelli:




**Dossier:** è l´insieme dei dati personali generati da eventi clinici presenti e trascorsi riguardanti il cittadino, che vengono condivisi tra i professionisti sanitari che lo assistono nell'ambito dell'ASST (ad es. ospedale, casa di comunità, casa di cura ecc.) per rendere più efficienti i processi di diagnosi e cura del paziente all´interno della struttura sanitaria e delle strutture del territorio, consentendo ai diversi professionisti che vi operano di accedere a tutte le informazioni cliniche relative ai precedenti interventi (ricoveri, visite ambulatoriali, accessi in pronto soccorso, valutazioni e PAI).

**Cartella Clinica Elettronica CCE**: è uno strumento di programmazione, gestione e verifica della cura fornita al paziente all'interno di un ambito ospedaliero di ricovero. Raccoglie le informazioni cliniche necessarie agli operatori sanitari per gestire il percorso di cura e acquisire gli esiti di sistemi diagnostici attivati all'interno della struttura ospedaliera, come Laboratorio (LIS) e Radiologia (RIS), e referti specialisti (AMB)

**Progetto individuale**: è uno strumento di programmazione, gestione e verifica che identifica e raccoglie i bisogni e le risposte cliniche socioassistenziali, riabilitative e di prevenzione per il cittadino. Si attiva all'accesso della persona ai punti di contatto di prossimità messi a disposizione dal sistema Territoriale. Il progetto traccia, orienta e supporta la persona e i professionisti nelle fasi di transizione tra i diversi setting di cura. La composizione del Progetto di Salute di ciascun individuo include i Piani

Assistenziali Individuali (PAI), eventuali Piani Riabilitativi Individuali (PRI) e tutta la documentazione sanitaria acquisita nell'ambito dell'assistenza territoriale del paziente.

## 8.2. Protezione dei dati personali

Il Regolamento UE n. 2016/679 del parlamento europeo e del consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (di seguito, anche il "Regolamento"), unitamente alla normativa nazionale di armonizzazione (D.lgs. 101/2018), il Codice della Privacy (D.lgs. 196/2003), nonché da ultimo, la L. 3 dicembre 2021, n. 205 di conversione in legge, con modificazioni, del decreto-legge 8 ottobre 2021, n. 139, concorrono, insieme ai provvedimenti emanati dall'Autorità Garante per la Protezione dei dati personali, a delineare il *framework* normativo concernente la protezione dei dati personali, idoneo a garantire che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, con particolare riferimento alla riservatezza, all'identità personale, nonché alla dignità dell'interessato.

La normativa richiamata prevede, in particolare, nella progettazione di un trattamento dei dati personali:

- La gestione mirata degli aspetti privacy del progetto, attraverso l'individuazione della veste giuridica degli attori coinvolti (ruoli privacy) e delle relative modalità di nomina (nel caso dei responsabili del trattamento);
- L'adozione di un approccio al trattamento *risk-based* volto a individuare misure di sicurezza tecniche e organizzative, tenuto conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, adeguate per garantire un livello di sicurezza adeguato al rischio, necessarie al fine di garantire un livello adeguato di protezione dei dati personali;
- L'adozione, con riguardo ai trattamenti di dati personali effettuati con l'ausilio di strumenti elettronici, di apposite istruzioni concernenti l'attribuzione delle

funzioni di amministratore di sistema (Provvedimento dell'Autorità Garante per la Protezione dei Dati personali del 27 novembre 2008 e ss.mm.ii., la cui validità non è revocata per effetto dell'entrata in vigore del Regolamento).

Vengono illustrati i requisiti minimi concernenti il rispetto della normativa della Privacy, che devono essere presi in considerazione nella progettazione e realizzazione del Sistema per la gestione digitale del territorio ai fini della completa *compliance* normativa del progetto.

Il tema della protezione dei dati personali assume un rilievo primario nello sviluppo progettuale: la messa a regime del Sistema per la gestione digitale del territorio comporterà infatti il trattamento su larga scala di dati "comuni" e di particolari categorie di dati personali (segnatamente, di dati idonei a rivelare lo stato di salute dell'interessato). In tale quadro di contesto, lo sviluppo tecnologico deve necessariamente essere improntato ai principi della protezione dei dati personali per impostazione predefinita (c.d. principio di *privacy by default*), e garantire che il trattamento abbia ad oggetto esclusivamente dati *adeguati, pertinenti e limitati* a quanto necessario rispetto alle finalità per le quali sono trattati (principio di minimizzazione dei dati).

Sotto tale prospettiva, le soluzioni tecnologiche a supporto dei processi digitali dovranno essere pensate considerando la protezione dei dati personali sin dalla fase della progettazione (principio di *privacy by design*), considerando la protezione dei dati personali come fulcro attorno al quale sviluppare la logica di progettazione.

Il progetto deve, inoltre - in ottemperanza di quanto sancito dall'art. 32 del Regolamento - prevedere l'implementazione di misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

- la pseudonimizzazione e la cifratura dei dati personali;
- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

- la previsione di una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Nel valutare l'adeguato livello di sicurezza, deve tenersi conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso non autorizzato a dati personali trasmessi, conservati o comunque trattati, occorso in modo accidentale o in conseguenza di azioni malevole di terzi.

Inoltre, con riguardo alle misure di sicurezza a protezione dei dati, l'evoluzione della disciplina relativa alla protezione dei dati personali, eventualmente mediante la pubblicazione di provvedimenti, regolamenti, ecc. ad hoc da parte dell'Autorità Garante, o per effetto della promulgazione di leggi o la pubblicazione di regolamenti ha già richiesto e potrebbe richiedere, in futuro, l'implementazione al trattamento di accorgimenti, standard di sicurezza, particolari configurazioni tecnologiche atte a garantire un livello di sicurezza delle informazioni superiore rispetto a quanto attualmente richiesto dalla normativa vigente.

Inoltre, ogni strumento telematico e ogni sistema informativo a supporto del trattamento dei dati personali deve essere progettato - in ogni caso - nel rispetto dei principi generali che ispirano il Codice in materia di protezione dei dati personali e del Regolamento. Deve, in particolar modo, essere valutata la pertinenza, la completezza e la non eccedenza dei dati trattati, nonché delle operazioni che si propone di eseguire su di essi rispetto alle finalità dei trattamenti in funzione delle attività assegnate.

Gli strumenti elettronici dovranno essere quindi configurati in modo da ridurre al minimo l'utilizzo di dati personali e dei dati identificativi, in modo da escluderne il trattamento ogni qual volta le finalità perseguite possano in concreto essere efficacemente perseguite attraverso dati anonimi (così come previsto dall'art. 11 del Regolamento) o mediante altre modalità che permettano di identificare l'interessato solo laddove strettamente necessario.

Inoltre, come previsto dal Regolamento, deve essere adottato un approccio basato sulla Security e Privacy by Design e by Default a tutela di tutto il ciclo di vita del trattamento dei dati personali, dal momento dell'acquisizione del dato alla sua

definitiva cancellazione (logica o fisica) o alla sua completa anonimizzazione. Tali accorgimenti potrebbero non essere definiti puntualmente dalla normativa applicabile in materia, ma dovranno essere individuati, durante la fase di progettazione attraverso specifiche attività di analisi dei rischi che i trattamenti di dati personali prospettano, analisi che includono la valutazione a monte dei potenziali impatti sui diritti e le libertà degli interessati.

Di seguito, vengono elencate i principali requisiti privacy che devono essere considerati nella progettazione del sistema di Gestione Digitale del Territorio:

- **Gestione degli accessi ai dati personali**

Il sistema deve prevedere l'accesso ai dati personali solo attraverso modalità digitali di autenticazione sicura degli operatori abilitati Riferimenti tecnici al paragrafo "9.3 Sicurezza – Controllo accessi logici".

- **Gestione dei privilegi assegnati ai profili di accesso**

Il sistema deve prevedere funzionalità avanzate di gestione dei profili autorizzativi di accesso ai dati e di abilitazione al compimento delle singole operazioni su di essi. Riferimenti tecnici al paragrafo "9.3 Sicurezza – Controllo accessi logici".

- **Funzionalità degli amministratori di sistema**

Il sistema deve prevedere funzionalità avanzate per la gestione dei profili attribuiti agli amministratori di sistema, prevedendo cruscotti e funzionalità di controllo. Riferimenti tecnici al paragrafo "9.3 Sicurezza – Controllo accessi logici".

- **Sistema automatizzato di Alert**

Il sistema deve prevedere la gestione di appositi avvisi (c.d. "Alert") scatenati automaticamente ed in "tempo reale" da eventi specifici predeterminati, quali, ad esempio, l'esecuzione di particolari operazioni sui dati personali che presentano un profilo di rischio significativo.

- **Tracciatura degli accessi ai dati personali**

Il sistema deve prevedere modalità automatizzate di tracciatura degli accessi ai dati personali idonee a garantire la verifica di integrità e non modificabili *ex post*, che registrino, a titolo esemplificativo, la/le operazione/i eseguita/e, il profilo che ha operato

sui dati, l'orario di accesso al sistema e traccino cronologicamente il compimento delle singole operazioni sui dati personali. Riferimenti tecnici al paragrafo "9.3 Sicurezza - Logging e monitoring".

- **Gestione di back up dei dati personali**

Implementazione di sistemi di back up dei dati in tempo reale, da garantire secondo i migliori standard applicabili al contesto e che garantiscano in ogni tempo la continua disponibilità delle informazioni, abbinati a sistemi di *business continuity* e di *disaster recovery*.

- **Funzionalità per la gestione dei tempi conservazione**

Previsione di un sistema automatizzato di gestione dei tempi di conservazione dei dati, agevolmente configurabile in funzione delle specifiche esigenze dei titolari del trattamento. Tale sistema, in particolare, deve consentire la cancellazione logica o la definitiva anonimizzazione dei dati personali in via automatica.

- **Procedure di verifica periodica delle autorizzazioni**

Implementazione di controlli atti alla verifica, in modo anche massivo, dei privilegi di accesso ai dati personali. "9.3 Sicurezza – Controllo accessi logici"

- **Verifiche di integrità delle informazioni**

Il sistema deve prevedere meccanismi atti a garantire e verificare l'integrità delle informazioni.

- **Protocolli di comunicazione sicura**

Utilizzo di protocolli sicuri di comunicazione dei dati personali adeguati ai migliori standard operativi di settore (a titolo esemplificativo, canali cifrati di comunicazione dei dati tra i soggetti coinvolti nei trattamenti). Riferimenti tecnici al paragrafo "9.3 Sicurezza - Network & Infrastructure Security".

- **Cifratura e separazione dei dati idonei a rivelare lo stato di salute dell'interessato**

Previsione di ambienti informatici destinati alla conservazione dei dati personali debitamente segregati in ragione della natura dei dati personali e degli specifici rischi informatici. Per la sicurezza delle informazioni, i dati personali dovranno inoltre essere

conservati all'interno di domini informatici cifrati, secondo criteri di cifratura avanzati e comunque adeguati alla natura delle informazioni trattate, nonché al contesto pubblicistico di riferimento, e comunque, che garantiscano livelli di sicurezza non inferiori ai migliori standard di settore.

- **Pseudonimizzazione dei dati personali**

Previsione di funzionalità di pseudonimizzazione dei dati personali ove richiesto in ragione delle specifiche esigenze del trattamento.

In particolare, i dati personali non dovranno più essere attribuibili a un interessato specifico senza l'utilizzo di informazioni aggiuntive, e tali informazioni aggiuntive dovranno essere conservate separatamente dai dati trattati e saranno soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuibili a una persona fisica identificata o identificabile.

- **Valutazione privacy preliminare**

Esecuzione, già dalla fase di definizione delle specifiche funzionali del progetto, di valutazioni di impatto del trattamento sui diritti e le libertà fondamentali degli interessati, che contemplino sia analisi dei rischi di sicurezza che il rispetto del principio di proporzionalità e necessità del trattamento.

## 8.3. Sicurezza

Vengono di seguito riportati, suddivisi per macro-ambito, i requisiti di sicurezza delle informazioni che il sistema per la Gestione Digitale del Territorio deve rispettare anche in ottica di integrazione e interazione con le altre componenti dell'ecosistema digitale regionale.

**Controllo accessi logici**

- L'accesso all'applicativo deve avvenire solo attraverso modalità digitali di autenticazione sicura degli operatori abilitati

- Devono essere implementati controlli autorizzativi che permettano di definire quali operazioni possa compiere uno specifico utente. A tal fine, i privilegi di accesso devono essere concessi nel rispetto dei principi di:
    - "Least Privilege": devono essere concessi all'utente esclusivamente i privilegi strettamente necessari a svolgere le attività per le quali è autorizzato;
    - "Need to Know": gli utenti devono essere autorizzati a trattare i soli dati essenziali allo svolgimento della loro mansione.

  La sussistenza dei requisiti di autorizzazione degli utenti deve essere verificata almeno semestralmente.
- Il sistema deve prevedere l'implementazione di controlli specifici sulle utenze con privilegi ampi per impedire operazioni illecite.
- Dev'essere periodicamente effettuata una revisione delle utenze profilate volta a disabilitare gli account non attivi (es. mancato log-on o relativi ad utenze cessate) e verificare la corretta assegnazione dei privilegi di accesso. Tale processo è richiesto per verificare la sussistenza dei requisiti di autorizzazione degli utenti.
- Tutte le utenze amministrative utilizzate per la gestione sistemistica devono essere gestite centralmente attraverso opportuni strumenti (es. IAM).

**Logging e monitoring**

- Devono essere previsti meccanismi e sistemi per la registrazione e memorizzazione dei log delle attività degli utenti (es. login, logout, ecc.).
- Devono essere previsti meccanismi e sistemi per la registrazione e memorizzazione dei log delle attività degli Amministratori di Sistema (es. login, logout, ecc.).
- Il sistema dev'essere integrato a strumenti per la registrazione ed il reporting di tutti gli eventi ed incidenti di sicurezza.
- I vari log generati dalla piattaforma devono essere raccolti all'interno di un sistema centralizzato che si occupa della correlazione degli eventi e dell'analisi di eventuali anomalie (es. SIEM, Log Management, piattaforme CASB).

- La piattaforma dev'essere soggetta a monitoraggio da parte di un centro altamente specializzato (CSOC) per l'individuazione di eventuali anomalie.
- Devono essere previsti meccanismi di protezione dei log in maniera da non poter essere cancellati da personale non autorizzato.

  I log raccolti devono essere protetti da un uso improprio (ad esempio manomissione in transito, accesso/modifica/cancellazione non autorizzati).

  Esempi di misure di sicurezza dei log memorizzati in locale ("at rest") sono:
  - memorizzare o copiare i log su storage in sola lettura;
  - autorizzare, registrare e monitorare tutti gli accessi ai log;
  - implementare meccanismi di rilevamento delle manomissioni, in modo da sapere se un record del log è stato modificato o eliminato;
  - rivedere periodicamente i privilegi per l'accesso ai log.

  Esempi di misure di sicurezza dei log in transito sono:
  - se i log sono inviati su reti non attendibili (ad esempio Internet), utilizzare un protocollo di trasmissione sicuro/ cifrato (ad esempio TLS);
  - effettuare controlli di due diligence (normativi e di sicurezza) prima di inviare i log a terze parti.
- Devono essere previsti dei meccanismi per la segregazione/il mascheramento dei dati degli Audit log al fine di renderli disponibili ai cittadini interessati o autorità giudiziarie senza compromettere altri cittadini in ambiente multitenant.
- Deve essere stabilito un limite temporale entro il quale possano essere conservati i log.
- È necessario configurare il protocollo NTP al fine di sincronizzare il clock del sistema.

**Protezione delle informazioni**

- Le informazioni trattate dall'applicativo devono essere opportunamente classificate, in accordo allo schema di classificazione delle informazioni adottato da Regione Lombardia e devono essere etichettate e censite in un inventario.
- Devono essere previsti meccanismi per la protezione dalla divulgazione non autorizzata delle informazioni riservate verso parti non autorizzate.

I meccanismi dovrebbero:

- identificare le informazioni riservate a rischio di divulgazione non autorizzata durante l'archiviazione;
- rilevare quando vengono divulgate informazioni riservate;
- sensibilizzare gli utenti della potenziale divulgazione non autorizzata di informazioni riservate;
- bloccare azioni dell'utente non autorizzate;
- essere configurati per raccogliere i risultati della scoperta e del rilevamento di eventuali incidenti, al fine di supportare le analisi.

- Devono essere mantenute aggiornate le mappature dei flussi di dati residenti all'interno del sistema.
- Devono essere implementate tecniche di data masking per minimizzare la visualizzazione di dati personali sulla base del principio del "need to know".
- Sulle macchine virtuali devono essere presenti strumenti di prevenzione e protezione come EDR, costantemente aggiornati.
- Devono essere implementati degli strumenti di prevenzione e protezione quale EDR sull'hypervisor. Il software EDR deve essere costantemente aggiornato.
- È necessario identificare le informazioni da sottoporre a cifratura per quanto riguarda:
  - i dati *at rest*;
  - i dati *in transit*;
  - i dati *in use*.
- Il ciclo di vita delle chiavi di cifratura/mascheramento dati (creazione, archiviazione, recupero, distribuzione, ritiro e distruzione) dev'essere gestito. Le chiavi non devono essere custodite nello stesso cloud in cui sono utilizzate ma dallo stesso consumer o da un provider specifico per il key management. La gestione e l'uso delle chiavi deve essere separata (Segregation of Duties).
- Il Provider del servizio cloud deve cifrare i dati "a riposo" (es. dati memorizzati nei database o nelle memorie di massa) e "in transito". La cifratura deve essere utilizzata al fine di:
  - proteggere la riservatezza delle informazioni sensibili o delle informazioni soggette a requisiti legali e normativi;

- determinare se le informazioni critiche sono state alterate (ad esempio implementando funzioni hash o la firma digitale).

Esempi di misure di sicurezza dei dati memorizzati in locale ("at rest") sono:

- memorizzare o copiare i log su storage in sola lettura;
- autorizzare, registrare e monitorare tutti gli accessi ai log;
- implementare meccanismi di rilevamento delle manomissioni, in modo da sapere se un dato è stato modificato o eliminato;
- rivedere periodicamente i privilegi per l'accesso ai dati.

Esempi di misure di sicurezza dei dati in transito sono:

- invio di informazioni cifrate;
- utilizzo di protocolli sicuri (es. HTTPS, SFTP, e canali VPN con IPSec o SSL -per tutte le connessioni dirette eseguite verso il servizio in Cloud);
- effettuare controlli di due diligence (normativi e di sicurezza) prima di inviare i dati a terze parti.

- La cifratura delle piattaforme e dei dati deve avvenire mediante algoritmi standard, open source e validati (es. AES-256). Dev'essere possibile, sulla base della valutazione di criticità del dato gestito, di implementare algoritmi di cifratura del dato basati sullo standard FIPS 140-2.
- Devono essere previsti dei controlli al fine di impedire che i dati di produzione siano replicati o usati in ambienti non di produzione (test e sviluppo).
- Il sistema e i dati devono essere protetti dall'accesso non autorizzato e dalla divulgazione delle informazioni effettuando l'hardening del sistema operativo.

**Crittografia**

- I dati devono essere accessibili tramite meccanismi di gestione delle chiavi crittografate centralizzati e sicuri. Le chiavi saranno allocate su apparati hardenizzati che dovranno garantire un principio di integrità e affidabilità.
- La crittografia dei "dati in transito", tramite l'utilizzo di protocolli sicuri come https, sftp, ftps, etc, rappresenta il livello di servizio minimo che deve essere garantito per tutto l'ecosistema.
- La crittografia dei "dati inattivi" implica l'implementazione di una soluzione orientata alla cifratura a livello di virtual machine e/o a livello di base dati. Tale

aspetto risulta basilare per rispondere alle esigenze di mitigazione dei rischi secondo le norme di privacy impact assessment.

- È necessario prevedere che i dati degli ambienti di produzione, pre-produzione vengano protetti tramite crittografia di file system, database.
- L'infrastruttura deve prevedere un servizio di conservazione sicura di tutte le chiavi di cifratura, siano master key, chiavi crittografate applicative.

**Business Continuity e Disaster Recovery**

- Esecuzione pianificata di copie di backup dei dati, delle configurazioni e delle immagini delle macchine su appositi supporti di memorizzazione.
- Deve essere periodicamente verificata l'utilizzabilità delle copie di backup mediante opportuni test di ripristino.
- Le copie di backup devono essere protette mediante opportune misure di sicurezza fisica e logica (e.g. cifratura delle copie in cloud, controllo accessi).
- Il Cloud Provider deve produrre un report di gestione del RPO (Recovery Point Objective) e del RTO (Recovery Time Objective).

**Change e Patch Management**

- Le modifiche devono essere implementate rispettando la politica di Change Management prevista da Regione Lombardia. Devono inoltre essere previste apposite procedure di rollback al fine di ripristinare lo stato iniziale di qualsiasi sistema o servizio in Cloud.
- Devono essere installate le patch di sicurezza sui sistemi per risolvere le vulnerabilità rilevate, in accordo con la procedura di patch management stabilita da Regione Lombardia.

**Network & Infrastructure Security**

- Devono essere implementate misure tecniche e tecniche di difesa in depth (es. deep packet analysis, traffic throttling, and black-holing) per l'individuazione e la riposta tempestiva ad attacchi basati su rete e associati con l'ingresso/uscita

di pattern di traffico specifiche (es. MAC spoofing and ARP poisoning attacks) e/o attacchi DDoS.

- I dispositivi di rete (inclusi router, switch e firewall) che costituiscono l'infrastruttura del servizio devono essere configurati opportunamente per:
    - evidenziare condizioni di sovraccarico o eccezioni, quando si verificano;
    - registrare gli eventi (logging) e salvarli su un sistema separato;
    - configurazione del protocollo NAT per i servizi esposti su rete e gestione delle regole di traduzione degli indirizzi IP;
    - integrarsi con meccanismi di controllo degli accessi (ad esempio per fornire autenticazione forte);
    - assicurare che le password non vengano inviate in chiaro;
    - disabilitare il "source routing", (tecnica di specificare all'interno dell'header IP il tragitto (route) che il pacchetto deve seguire per mantenere il controllo all'interno del dispositivo di inoltro dei pacchetti.
- Devono essere previsti dei Web Application Firewall per la protezione del sistema.
- Devono essere implementate opportune logiche di ridondanza applicativa e/o infrastrutturale.
- La configurazione delle porte, dei protocolli e dev'essere ristretta in funzione delle attività fondamentali da svolgere e rivista periodicamente in termini di adeguatezza.
- Le reti e le istanze virtuali devono essere progettate e configurate per limitare e monitorare il traffico tra connessioni affidabili ("trusted") e non attendibili ("untrusted"). Tali configurazioni devono essere riviste almeno una volta all'anno.
- Le prestazioni dell'applicazione devono essere monitorate. Il monitoraggio comporta la raccolta e l'analisi dei dati per determinare le prestazioni, l'integrità e la disponibilità dell'applicazione. Una strategia di monitoraggio efficace aiuta a comprendere il funzionamento dettagliato dei componenti dell'applicazione, e ciò permette di rilevare le anomalie che potrebbero essere correlate alla sicurezza del codice o potenziali attacchi.
- Devono essere limitati gli indirizzi IP di origine in ingresso.

- Le interfacce di gestione della macchina virtuale nei servizi ibridi PaaS e IaaS devono essere protette usando un'interfaccia di gestione che consenta all'utente di gestire direttamente in remoto le macchine virtuali: non abilitare l'accesso remoto diretto alle macchine virtuali da Internet.
- È opportuno adottare un modello di sicurezza "Zero Trust".
- Il traffico di rete trasmesso tra le varie componenti dell'ecosistema digitale deve essere cifrato utilizzando protocolli di comunicazione sicura per tutti i dati in transito sulle reti, come ad esempio HTTPS, SFTP, e canali VPN con IPSec o SSL.
- Devono essere implementati sistemi e dispositivi anti-DDOS per la protezione da attacchi aventi come obiettivo l'indisponibilità di uno o più servizi.
- Il provider del servizio cloud deve utilizzare un protocollo di rete sicuro per l'import/export dei dati e per la gestione del servizio. Deve inoltre, fornire un documento per dettagliare gli standard di interoperabilità e portabilità adottati. In particolare, il provider deve fornire:
    - procedure e API per l'esportazione dei dati dal cloud;
    - formati di esportazione interoperabili;
    - possibilità di procedere autonomamente all'esportazione dei dati.
- La migrazione delle informazioni e dei dati da server fisici e applicazioni a server virtuali richieste un canale di comunicazione sicuro e cifrato.
- Il provider del servizio cloud deve utilizzare delle piattaforme e formati di virtualizzazione standard (es. OVF) per garantire l'interoperabilità e deve documentare modifiche customizzate effettuate su qualsiasi hypervisor in uso e gli eventuali hook di virtualizzazione specifici della soluzione.
- Deve essere implementato un meccanismo di sandboxing per proteggere la piattaforma PaaS fornita dal provider del servizio cloud. Tale piattaforma deve essere monitorata dal provider al fine di gestire e rimediare ad eventuali bug e vulnerabilità.

**Vulnerability Management**

- Devono essere schedulate attività periodiche effettuate da sonde in grado di rilevare vulnerabilità sul sistema (Vulnerability Assessment).

- Devono essere svolte attività di analisi di sicurezza mirate, con lo scopo di rilevare vulnerabilità e simulare attacchi informatici (Penetration Test). I Penetration Test devono essere resi una parte standard del processo di compilazione e distribuzione dell'applicazione.

**Sviluppo Sicuro**

- L'applicazione dev'essere sviluppata se le regole e le tecniche dettate da OWASP.
- L'applicazione dev'essere sviluppata utilizzando librerie sicure.
- Dev'essere utilizzata la modellazione delle minacce durante la progettazione dell'applicazione.
- E' necessario garantire la separazione fisica o virtuale degli ambienti che compongono il sistema (es. sviluppo, test, formazione, produzione). Gli ambienti di esercizio possono essere separati da quelli di sviluppo e collaudo utilizzando domini di rete differenti, segregandoli fisicamente o logicamente (es. mediante VLAN). Il perimetro dei differenti domini deve essere controllato mediante dei gateway appositi (es. un firewall).
- Devono essere svolte attività di code review durante lo sviluppo dell'applicativo.

**Sicurezza Applicativa**

- Le interfacce applicative (API) tra i vari componenti devono essere progettate, sviluppate, implementate e testate in conformità con i principali standard del settore (ad esempio OWASP per le applicazioni Web) e rispettare gli obblighi di conformità legali o normativi applicabili.
- Sulle interfacce applicative e sui database devono essere implementati dei controlli di integrità sugli input e sugli output dei dati (ad esempio riconciliazione dei dati) per impedire errori di elaborazione manuali o sistematici, corruzione di dati o uso improprio. Tale controllo dev'essere eseguito anche in caso di download/upload di file.
- Dev'essere implementata la validazione degli input impedendo la possibilità di sfruttare vulnerabilità comuni.

- Devono essere utilizzati opportuni strumenti di verifica dell'integrità dei file per assicurare che i file critici di sistema (compresi eseguibili, librerie e file di configurazione) non siano stati alterati. Nel caso in cui la verifica venga eseguita da uno strumento automatico, per qualunque alterazione di tali file deve essere generato un alert.

  Per il supporto alle analisi, il sistema di segnalazione deve essere in grado di mostrare la cronologia dei cambiamenti della configurazione nel tempo e identificare chi ha eseguito ciascuna modifica.

  I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.

**Analisi dei rischi**

In ottemperanza alle normative vigenti, deve essere svolta una analisi dei rischi antecedente la messa in produzione del servizio e all'introduzioni di modifiche rilevanti allo stesso, che evidenzi almeno i seguenti punti:

- i rischi associati all'erogazione del suddetto servizio in cloud;
- il grado di rischio associato ad ogni rischio identificato;
- le contromisure tecnico/organizzative a mitigazione del rischio identificato;
- il valore di rischio atteso a valle dell'applicazione delle contromisure;
- la proposta di accettazione del rischio per quegli aspetti per i quali non sia possibile in alcun modo mitigare i rischi.