IRE ISTITUTO NAZIONALE TUMORI REGINA ELENA ISG ISTITUTO DERMATOLOGICO SAN GALLICANO
ISTITUTI DI RICOVERO E CURA A CARATTERE SCIENTIFICO

DELIBERAZIONE N. **1043** DEL **30/11/2023**

OGGETTO: Approvazione del Piano per la transizione digitale dei servizi amministrativi e sanitari degli IFO per il triennio 2024 - 2026

Esercizi/o e conto 2024/2026 Centri/o di costo . **- Importo presente Atto: € .** **- Importo esercizio corrente: € .** Budget **- Assegnato: € -** **- Utilizzato: € -** **- Residuo: € -** **Autorizzazione n°: -** Servizio Risorse Economiche: **Francesca Romana Benedetto**	STRUTTURA PROPONENTE **UOSD Ingegneria Clinica e Tecnologie e Sistemi Informatici** Il Dirigente Responsabile **Giuseppe Navanteri** Responsabile del Procedimento **Giuseppe Navanteri** L'Estensore **Silvia Placidi** Proposta n° DL-1070-2023
PARERE DEL DIRETTORE SANITARIO Positivo Data 30/11/2023 IL DIRETTORE SANITARIO **Ermete Gallo**	**PARERE DEL DIRETTORE AMMINISTRATIVO** Positivo Data 30/11/2023 IL DIRETTORE AMMINISTRATIVO **Laura Figorilli**

Parere del Direttore Scientifico IRE **Gennaro Ciliberto** data 27/11/2023 Positivo

Parere del Direttore Scientifico ISG ad interim **Gennaro Ciliberto** data 27/11/2023 Positivo

La presente deliberazione si compone di n° 12 pagine e dei seguenti allegati che ne formano parte integrante e sostanziale:
Allegato 1 composto da num. 48 pagine

Visto il decreto legislativo 30.12.1992, n. 502 e successive modificazioni ed integrazioni;

Visto il decreto legislativo 16.10.2003, n. 288;

Vista la legge regionale 23.01.2006, n. 2;

Visto l'Atto Aziendale adottato con deliberazione n. 153 del 19.02.2019 ed approvato dalla Regione Lazio con DCA n. U00248 del 2.07.2019, modificato e integrato con la delibera 1254 del 02.12.2020, n.46 del 21/01/2021 e n.380 del 25/03/2021, approvate dalla Direzione Salute ed Integrazione Sociosanitaria della Regione Lazio, con Determinazione n.G03488 del 30/03/2021;

Visto il Decreto del Presidente della Regione Lazio n. T00200 del 29.10.2021 avente ad oggetto: "Nomina del Direttore Generale dell'IRCCS IFO-Istituti Fisioterapici Ospitalieri";

Vista la deliberazione n.1123 del 02.11.2021 di insediamento ed assunzione in carica del Direttore Generale degli Istituti Fisioterapici Ospitalieri di Roma Dott.ssa Marina Cerimele;

Viste le deliberazioni n. 212 del 16.03.2022 e n. 154 del 28.02.2022 con le quali sono stati nominati rispettivamente la Dott.ssa Laura Figorilli quale Direttore Amministrativo ed il Dott. Ermete Gallo quale Direttore Sanitario degli Istituti Fisioterapici Ospitalieri;

Premesso che l'informatica nella pubblica amministrazione si pone quale strumento cardine per accrescere la trasparenza amministrativa che, costituendo principio fondamentale del diritto amministrativo, trasversalmente interessa tutti gli am-

biti strategici dell'Amministrazione nell'ottica di una maggiore efficienza, efficacia ed economicità;

che il Codice dell'Amministrazione Digitale (DLGS. n. 82/2005 e s.m.i.) ha tracciato il quadro normativo entro cui deve attuarsi la digitalizzazione della Pubblica Amministrazione;

che le successive modifiche introdotte dal DL 235/2010, hanno poi avviato un ulteriore processo verso una PA moderna, digitale e sburocratizzata;

Atteso che l'art. 14.bis comma 2 del CAD "Agenzia per l'Italia Digitale (AgID)", prevede che AgID ogni anno emani il Piano triennale per l'informatica nella pubblica amministrazione, da approvarsi entro il 30 settembre di ogni anno dal Presidente del Consiglio dei ministri o dal Ministro delegato, contenente la fissazione degli obiettivi e l'individuazione dei principali interventi di sviluppo e gestione dei sistemi informativi delle pubbliche amministrazioni;

che l'art. 17 del D.Lgs. 7.3.2005 n. 82 - Codice dell'Amministrazione Digitale (aggiornato con le modifiche e integrazioni introdotte dal Decreto Legislativo n. 217 del 13.12.2017), rubricato "Responsabile per la transizione al digitale e difensore Civico", attribuisce al Responsabile per la transizione al digitale compiti di coordinamento e di impulso ai processi di reingegnerizzazione dei servizi, quali in particolare:

- *migrazione di tutti gli applicativi al cloud;*
- *coordinamento strategico dello sviluppo dei sistemi informativi, di teleco municazioni e fonia;*
- *indirizzo e coordinamento dello sviluppo dei servizi, sia interni che esterni, forniti dai sistemi informativi di telecomunicazione e fonia dell'amministrazione;*

- *indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza in- formatica relativamente ai dati, ai sistemi e alle infrastrutture anche in relazione al sistema pubblico di connettività;*

- *accesso dei soggetti disabili agli strumenti informatici e promozione della accessibilità;*

- *analisi periodica della coerenza tra l'organizzazione dell'amministrazione e l'utilizzo delle tecnologie dell'informazione e della comunicazione, al fine di migliorare la soddisfazione dell'utenza e la qualità dei servizi nonché' di ridurre i tempi e i costi dell'azione amministrativa;*

- *cooperazione alla revisione della riorganizzazione dell'amministrazione;*

- *indirizzo, coordinamento e monitoraggio della pianificazione prevista per lo sviluppo e la gestione dei sistemi informativi di telecomunicazione e fonia;*

- *progettazione e coordinamento delle iniziative rilevanti ai fini di una più efficace erogazione di servizi in rete a cittadini e imprese mediante gli strumenti della cooperazione applicativa tra pubbliche amministrazioni, ivi inclusa la predisposizione e l'attuazione di accordi di servizio tra amministrazioni per la realizzazione e compartecipazione dei sistemi informativi cooperativi;*

- *promozione delle iniziative attinenti all'attuazione delle direttive impartite dal Presidente del Consiglio dei Ministri o dal Ministro delegato per l'innovazione e le tecnologie;*

- *pianificazione e coordinamento del processo di diffusione, all'interno della amministrazione, dei sistemi di identità e domicilio digitale, posta elettronica, protocollo informatico, firma digitale o firma elettronica qua-*

lificata e mandato informatico, nonché delle norme in materia di accessibilità e fruibilità.

Vista la Circolare n. 3 del 1° Ottobre 2018 del Ministro della Pubblica Amministrazione la quale invita tutte le amministrazioni ad individuare al loro interno un Ufficio per la Transizione al Digitale e un Responsabile quale figura di riferimento e punto di contatto con l'Agenzia per l'Italia Digitale e la Presidenza del Consiglio dei Ministri, per le questioni connesse alla trasformazione digitale delle Pubbliche Amministrazioni, nonché per la partecipazione a consultazioni e censimenti previsti;

Considerato che con Deliberazione n. 185 del 16 febbraio 2021 si è individuata l'UOSD Ingegneria Clinica e Tecnologie e Sistemi Informatici quale Ufficio referente per la transizione digitale degli IFO e, contestualmente, si è nominato l'Ing. Giuseppe Navanteri, Responsabile della UOSD Ingegneria Clinica e Tecnologie e Sistemi Informatici, come Responsabile per la transizione al digitale che, tra le principali funzioni, svolge quella di garantire operativamente la trasformazione digitale degli Istituti, coordinandola nello sviluppo dei servizi pubblici digitali e nell'adozione di modelli di relazione trasparenti e aperti con i cittadini.;

Dato atto che gli IFO hanno predisposto un documento programmatico valido per il triennio 2018-2020 e inerente all'attività informatica sanitaria ed amministrativa, approvato con Determinazione n. 1019 del 7 dicembre 2017 ed un secondo piano per la transizione al digitale per il triennio 2021-2023 con deliberazione IFO n. 486 del 23/04/2021;

Ravvisato l'art. 12 comma 1 del CAD "Norme generali per l'uso delle tecnologie dell'informazione e delle comunicazioni nell'azione amministrativa" con cui si prevede che le PA sono tenute, nel rispetto della loro autonomia, a realizzare azioni in conformità con gli obiettivi indicati nel Piano nazionale triennale per l'informatica nella pubblica amministrazione;

Preso atto che il Piano Triennale per l'informatica costituisce strumento essenziale per promuovere la trasformazione digitale dell'Ente;

che il Piano triennale rappresenta la naturale evoluzione di quanto descritto nei precedenti piani e di tutte le attività che l'UOSD Ingegneria Clinica e Tecnologie e Sistemi Informatici ha attuato in termini di informatizzazione e digitalizzazione;

che il Piano è redatto in conformità a quanto indicato dal Piano Triennale per l'Informatica della Pubblica Amministrazione dell'Agenzia per l'Italia Digitale e, specificatamente, con quanto indicato all'art. 9 "Indicazioni per le pubbliche amministrazioni";

che tale Piano (Allegato 1 alla presente a formarne parte integrante e sostanziale) deve porsi come obiettivo quello di declinare la visione strategica ed i modelli che guideranno la transizione al digitale e l'evoluzione dell'ICT degli IFO nel prossimo triennio;

che, coerentemente con gli obiettivi definiti per il Legislatore dall'Agenzia per l'Italia Digitale, il Piano vuole dare una notevole accelerazione al processo di semplificazione amministrativa e di digitalizzazione sia semplificando le relazioni con cittadini e imprese attraverso l'uso competitivo delle tecnologie dell'informazione e della comunicazione (ICT), sia attraverso la ricerca di un miglioramento continuo dei processi interni dell'Ente;

Accertato che tale Piano si colloca in un contesto strategico in fase di continua evoluzione, caratterizzato da una elevata dinamicità in considerazione anche degli impulsi che continuano a pervenire dal mondo della tecnologia, soprattutto per quanto riguarda l'Intelligenza Artificiale, la robotica e i Big Data;

che Dati, Cloud e IA sono tasselli indispensabili da inserirsi nel sedimento infrastrutturale costituito dalle tecnologie 5G incrementando in tal senso, in modo esponenziale, i benefici e mettendo a disposizione canali comunicativi con elevate caratteristiche di performance;

che il Piano presente si pone in continuità con le versioni precedenti e con il Modello strategico di AgID adeguando i principi base alle mutate condizioni dello scenario normativo e tecnologico:

• Digital per default

• Cloud first

• Once only

• Speed only

Accertato che gli IFO intendono progredire nel percorso di digitalizzazione e di innovazione avviando iniziative atte a:

- migliorare la relazione con gli assistiti attraverso il ricorso a strumenti/tecnologie che tendano ad aumentare la consapevolezza degli stessi nei percorsi di cura e ad abbattere le distanze con la struttura sanitaria e il suo personale;

- migliorare le performance complessive degli Istituti attraverso una più incisa governance che riesca tramite la gestione ottimale del patrimonio informativo a ridurre le liste di attesa, ottimizzare l'uso dei posti letto, diminuire il

tempo amministrativo di ogni medico a vantaggio del tempo di cura, incrementare l'efficacia chirurgica con l'ausilio della robotica e di altre innovazioni;

che il Piano si incentra in particolare sul recepimento della Strategia Cloud Italia, dettata dal Dipartimento per la trasformazione digitale e dall'Agenzia per la cybersicurezza nazionale (ACN), che contiene gli indirizzi strategici per il percorso di migrazione verso il Cloud di dati e servizi digitali della Pubblica Amministrazione;

che i principali obiettivi di digitalizzazione del triennio sono i seguenti:

- Migrazione al Cloud delle componenti tecnologiche operanti in ambito di rete degli IFO e inserite nel Piano di Migrazione predisposto anche in base alle indicazioni fornite dalla Regione Lazio con comunicazione prot. nr. 505366 del 10 maggio 2023 (anni 2023 – 2024);

- Nuova Governance in Cloud del sistema informativo ospedaliero (anni 2024 – 2025);

- Potenziamento dell'infrastruttura in fibra ottica per i collegamenti dorsali e di piano (anni 2024 – 2026);

- Estensione della Piattaforma di workflow management finalizzata alla digitalizzazione dei consensi informati e del consenso informato privacy presso tutti i reparti ed ambulatori degli IFO (anni 2024 – 2026);

- Integrazione della Piattaforma di workflow management finalizzata alla digitalizzazione dei consensi informati e del consenso informato privacy al fine di costituire la cartella clinica di reparto dell'assistito (anni 2023 – 2026);

- Avvio ed estensione del sistema di indoor navigator per guidare il paziente e gli eventuali accompagnatori all'interno delle strutture degli IFO (anni 2024 – 2026);

- Evoluzione del sistema di conservazione digitale a norma sia in ambito sanitario sia in ambito amministrativo (anni 2024 – 2026);

- Evoluzione del sistema di sottoscrizione digitale a norma sia in ambito sanitario sia in ambito amministrativo (anni 2024 – 2026);

- Alimentazione del fascicolo sanitario elettronico 2.0 attraverso l'interfacciamento dei sistemi operanti in IFO (anni 2024 – 2026);

- Evoluzione del sistema di business intelligence del sistema informativo ospedaliero (anni 2023 – 2026);

- Potenziamento ed evoluzione del sistema di sicurezza informatica (anni 2023 – 2025);

- Evoluzione del sistema amministrativo-contabile (anni 2023 – 2026);

- Evoluzione del sistema di gestione delle risorse umane (anni 2023 – 2026);

- Evoluzione del sistema di gestione degli atti e del protocollo informatico (anni 2023– 2026);

- Ammodernamento del parco tecnologico ospedaliero da effettuarsi anche con il ricorso alle risorse PNRR (anni 2023 – 2026);

- Evoluzione del Portale aziendale attraverso manutenzione del sito internet e implementazione di una soluzione in grado di gestire e veicolare internamente il flusso delle informazioni organizzandole secondo logiche colla-

borative permettendo una più sicura connessione dall'esterno della rete aziendale (anni 2023 – 2026);

- Evoluzione della Piattaforma di telemedicina, televisita e telemonitoraggio per l'attivazione di servizi di assistenza verso gli assistiti;

- Evoluzione del sistema informativo ospedaliero;

Rilevato che il Piano rappresenta quindi la sintesi di un percorso nel quale le risorse aziendali convergono per conseguire l'obiettivo di ridurre la burocrazia, migliorare la qualità dei servizi offerti, semplificare il rapporto con i propri utenti e realizzare infrastrutture e piattaforme abilitanti ad una visione organizzata e sistemica dell'azienda;

Ritenuto pertanto, necessario procedere all'approvazione del Piano Triennale ICT 2024 - 2026, dando altresì atto che dall'adozione del presente provvedimento non discende direttamente alcun onere di spesa e che i singoli interventi che lo compongono, saranno oggetto di specifici provvedimenti in cui saranno individuati i relativi oneri finanziari;

Attestato che il presente provvedimento, a seguito dell'istruttoria effettuata, nella forma e nella sostanza è totalmente legittimo e utile per il servizio pubblico, ai sensi dell'art. 1 della legge 20/94 e successive modifiche, nonché alla stregua dei criteri di economicità e di efficacia di cui all'art. 1, primo comma, della legge 241/90, come modificata dalla legge 15/2005.

Propone

Per i motivi di cui in narrativa che si intendono integralmente confermati:

- Di approvare il Piano per la transizione digitale dei servizi amministrativi e sanitari per il triennio 2024 - 2026 di cui all'Allegato 1 alla presente deliberazione a formarne parte integrane e sostanziale, dando altresì atto che, dall'adozione del presente provvedimento non discende direttamente alcun onere di spesa, e che i singoli interventi che lo compongono saranno oggetto di specifici provvedimenti in cui saranno individuati i relativi oneri finanziari.

La UOSD proponente curerà tutti gli adempimenti per l'esecuzione della presente deliberazione

Il Dirigente della UOSD Ingegneria Clinica e Tecnologie e Sistemi Informatici

Giuseppe Navanteri

Il Direttore Generale

Visto il Decreto Legislativo 30.12.1992, n. 502 e successive modificazioni ed integrazioni;

Vista la Legge Regionale 23.01.2006, n. 2;

Visto l'Atto Aziendale adottato con deliberazione n. 153 del 19.02.2019 e approvato dalla Regione Lazio con DCA n. U00248 del 2.07.2019, modificato e integrato con deliberazioni n. 1254 del 02.12.2020, n. 46 del 21/01/2021 e n. 380 del 25.03.2021, approvate dalla Direzione Salute ed Integrazione Sociosanitaria della Regione Lazio, con Determinazione n. G03488 del 30.03.2021;

In virtù dei poteri conferitigli con Decreto del Presidente della Regione Lazio n. T00200 del 29.10.2021.

Preso atto che il Dirigente proponente il presente provvedimento, sottoscrivendolo, attesta che lo stesso a seguito dell'istruttoria effettuata, nella forma e nella sostanza è totalmente legittimo e utile per il servizio pubblico, ai sensi dell'art. 1 della legge 20/94 e s.m.i., nonché alla stregua dei criteri di economicità e di efficacia di cui all'art. 1, primo comma, della legge 241/90, come modificata dalla legge 15/2005.

Visto il parere favorevole del Direttore Amministrativo e del Direttore Sanitario Aziendale;

ritenuto di dover procedere;

Delibera

di approvare la proposta così formulata concernente *"Approvazione del Piano per la transizione digitale dei servizi amministrativi e sanitari degli IFO per il triennio 2024 - 2026"* e di renderla disposta.

Il Direttore Generale

Dr.ssa Marina Cerimele

Documento firmato digitalmente ai sensi del D.Lgs 82/2005 s.m.i. e norme collegate

SISTEMA SANITARIO REGIONALE
IRCCS
ISTITUTI FISIOTERAPICI
OSPITALIERI

IRE ISTITUTO NAZIONALE TUMORI REGINA ELENA
ISG ISTITUTO DERMATOLOGICO SAN GALLICANO
ISTITUTI DI RICOVERO E CURA A CARATTERE SCIENTIFICO

Piano Triennale per la transizione digitale 2024-2026 degli Istituti Fisioterapici Ospitalieri (IFO)

Riferimento al Piano Triennale per l'informatica 2022-2024 pubblicato da AGID

Il Responsabile UOSD
Ingegneria Clinica e Tecnologie
e Sistemi Informatici
Responsabile per la Transizione
al Digitale

Roma, 21/11/2023

Ing. Giuseppe Navanteri

Sommario

PARTE Iª - IL PIANO TRIENNALE

Introduzione

Gli Istituti Fisioterapici Ospitalieri (IFO) di Roma sono un Ente di diritto pubblico istituiti con R.D. del 4/8/1932 n. 1296 e comprendono gli Istituti di Ricovero e Cura a Carattere Scientifico (IRCCS) riconosciuti con D.M. 22/2/1939:

- Regina Elena IRE, per la ricerca, lo studio e la cura dei tumori;
- San Gallicano ISG, per la ricerca, lo studio e la cura delle dermopatie anche oncologiche e professionali e delle malattie sessualmente trasmesse.

La sede degli Istituti è stabilita in Roma, in Via Elio Chianesi n. 53.

Il sito Istituzionale è raggiungibile all'indirizzo web: http//www.ifo.it e l'indirizzo di Posta Elettronica Certificata pubblicata sull'IndicePA è: aagg@cert.ifo.it.

Le linee di indirizzo programmatico degli IFO in ambito di trasformazione digitale si collocano nell'ambito di una qualsiasi azienda ospedaliera che svolge servizio pubblico in coordinamento con l'ente regionale di competenza.

Il contesto legislativo è quindi definito dalla normativa nazionale e regionale di riferimento, comprendendo anche le linee di indirizzo/strategiche/direttive emanate da:

- ✓ Ministero della Salute
- ✓ Istituto Superiore della Sanità
- ✓ Regione Lazio
- ✓ Il Garante per la Protezione dei Dati Personali

A livello comunitario e a livello mondiale, invece hanno rilevo gli atti di indirizzi/studi/report dell'Organizzazione Mondiale della Sanità e dei Regolamenti emanati dell'Unione Europea atti normativi a carattere generale, vincolanti e direttamente applicabili senza bisogno di atti di recepimento (art. 249, par. 2, TCE) e, quindi, senza che sia necessario un intervento formale delle autorità nazionali, a meno che non sia richiesto dallo stesso Regolamento.

La scorsa edizione del Piano, dal punto di vista tecnico, poneva evidenza sulle azioni per il recepimento del vigente Piano Triennale per l'Informatica con riferimento in particolare al Modello strategico dell'informatica nella PA e sulla descrizione del Modello organizzativo di Sicurezza Informatica adottato dagli Istituti.

L'attuale si incentra in particolare sul recepimento della ***Strategia Cloud Italia***, dettata dal Dipartimento per la trasformazione digitale e dall'Agenzia per la cybersicurezza nazionale (ACN), che contiene gli indirizzi strategici per il percorso di migrazione verso il Cloud di dati e servizi digitali della Pubblica Amministrazione.

Si allinea alle indicazioni contenute dal **Piano Triennale per l'informatica 2022-2024** pubblicato da AGID.

In relazione, inoltre, alle attività previste con l'obiettivo di sostenere importanti Riforme e Investimenti a beneficio del nostro Servizio Sanitario Nazionale e dei cittadini da realizzare attraverso il **Piano nazionale di ripresa e resilienza** (PNRR) dell'Unione Europea che rappresenta lo strumento cardine del programma Next Generation EU, nel presente documento si illustrano le azioni IT che sono previste in tale ambito e nel correlato **Piano nazionale per gli investimenti complementari** (PNC) di competenza del Ministero della salute.

Come noto, Il PNRR ha destinato alla Missione Salute € 15,63 miliardi, pari all'8,16% dell'importo totale, per sostenere importanti riforme e investimenti a beneficio del Servizio sanitario nazionale, da realizzare entro il 2026. Ma complessivamente le risorse straordinarie per l'attuazione del PNRR e il rinnovamento della sanità pubblica italiana superano i 20 miliardi di euro. Tra queste, le risorse introdotte dall'Italia con il Piano nazionale per gli investimenti complementari al PNRR (PNC), che destina alla salute ulteriori 2,89 miliardi di euro.

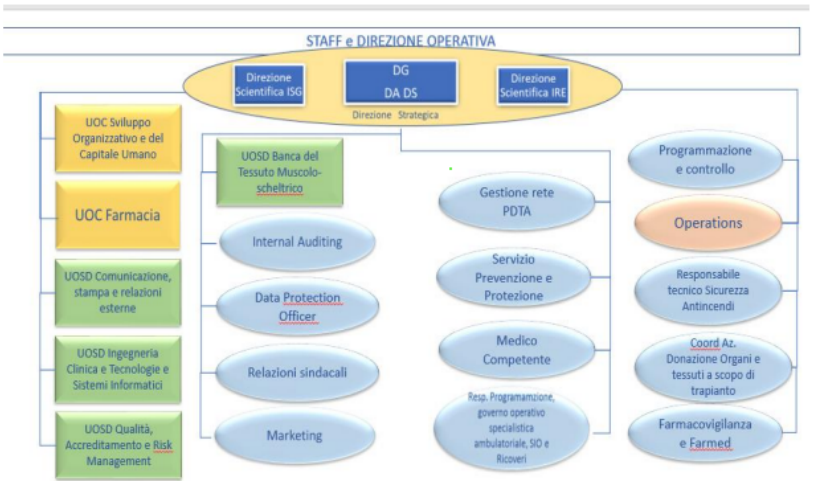
Per quanto premesso, le attività del Piano Triennale si inseriscono nell'ambito della strategia nazionale di favorire lo sviluppo di una società full digital, che ponga i cittadini (nel contesto sanitario, gli assistiti) al centro delle azioni utilizzando al meglio le opportunità offerte dai digital enabler per la digitalizzazione della Sanità Pubblica incentivando la standardizzazione e l'innovazione dei servizi con approcci del tipo privacy e security by design.

Ruolo del Responsabile per la Transizione al Digitale

Con Deliberazione n. 185 del 16.02.2021, in aderenza a quanto previsto dall'articolo 17 del Codice dell'Amministrazione Digitale, l'Ufficio per la transizione alla modalità digitale è stato individuato nell'UOSD Ingegneria Clinica e Tecnologie e Sistemi Informatici a cui competono quindi "*le attività e i processi organizzativi necessari alla realizzazione di un'amministrazione digitale e all'erogazione di servizi fruibili, utili e di qualità*".

Il Responsabile della UOSD, Ing. Giuseppe Navanteri, è il Responsabile per la Transizione al Digitale (RTD) e, tra le principali funzioni, svolge quella di garantire operativamente la trasformazione digitale degli Istituti, coordinandola nello sviluppo dei servizi pubblici digitali e nell'adozione di modelli di relazione trasparenti e aperti con i cittadini.

La citata UOSD si incardina nell'organo di Staff e di Direzione Operativa, a supporto della Direzione Strategica degli Istituti.



La UOSD Ingegneria Clinica e Tecnologie e Sistemi Informatici gestisce il patrimonio tecnologico ed ICT degli IFO. Ha il compito di gestire il parco tecnologico degli IFO garantendo l'uso sicuro, appropriato ed economico, nel rispetto delle normative tecnico/legali vigenti di tutte le apparecchiature elettromedicali, mediche e scientifiche.

Ha l'importante funzione di supporto tecnico/ingegneristico agli operatori sanitari per la valutazione di nuove acquisizioni in tecnologia (anche attraverso l'Hospital Based Health Technology Assessment), per la risoluzione dei guasti alle apparecchiature e per la ricerca di

nuovi percorsi clinico assistenziali che aumentino l'efficacia diagnostica e/o terapeutica grazie all'utilizzo delle nuove tecnologie presenti sul mercato.

Visto il legame sempre più stretto tra apparecchiature e sistemi informatici, la stessa UOSD è deputata a presidiare i flussi informativi a supporto di tutti i processi dell'ospedale.

È responsabile della definizione dell'architettura ICT aziendale, delle nuove scelte tecnologiche, applicative o di sourcing e della relativa allocazione delle risorse economiche.

Al riguardo, l'UOSD è responsabile delle attività di declinazione degli obiettivi strategici dettati dai vari Piano aziendali in obiettivi IT.

In tale prospettiva è di conseguenza necessario l'allineamento dei vari documenti strategici emanati dagli IFO. Può, al riguardo, essere utile definire un albero della performance come mappa logica che rappresenti graficamente i legami tra la missione, le aree strategiche, gli obiettivi strategici, le iniziative progettuali di supporto e i relativi indicatori di outcome.

Il Presente Piano è dunque la rappresentazione di come gli obiettivi di diversa natura possano fornire contributi all'interno di un disegno strategico complessivo coerente.

Contesto Strategico

Il Piano si colloca in un contesto strategico in fase di continua evoluzione, caratterizzato da una elevata dinamicità in considerazione anche degli impulsi che continuano a pervenire dal mondo della tecnologia, soprattutto per quanto riguarda l'Intelligenza Artificiale, la robotica e i Big Data.

E' innegabile che già con la pandemia si era registrato un forte incremento della digitalizzazione dei processi sanitari, con le possibilità offerte dal PNRR è in atto una ulteriore spinta che consentirà di disporre di una mole di dati sempre più ampia.

Occorrono pertanto tecnologie all'avanguardia che consentano di navigare tra i dati, mettendoli in relazione tra loro e cercando di accrescerne la loro semantica attraverso processi di elaborazione cognitiva digitale ed al contempo un sistema sempre più articolato di cybersecurity che permetta un uso sicuro delle risorse.

In questo senso, sono innumerevoli le opportunità messe a disposizione con i processi di migrazione al Cloud dei sistemi informativi delle Asl, delle Aziende Ospedaliere e delle piattaforme sanitarie delle Regioni.

Il ricorso a tecniche di Intelligenza Artificiale, unitamente a strumenti anche basilari di Chatbot, si sta imponendo come una nuova modalità di interazione tra mondo sanitario e assistiti, anche se al riguardo è bene sottolineare come un processo non controllato e senza regole possa costituire un possibile vulnus nella gestione dei dati sensibili.

A tal proposito si ritiene utile citare il rapporto "*Ethics and Governance of Artificial Intelligence for Health*" [1] realizzato dall'**Organizzazione Mondiale della Sanità** nel giugno 2021, che, in relazione all'uso dell'IA in ambito sanitario, ne descrive in modo dettagliato rischi e opportunità.

Dati, Cloud e IA sono tasselli che devono poi inserirsi nel sedimento infrastrutturale costituito dalle tecnologie 5G, che incrementano in modo esponenziale i benefici mettendo a disposizione canali comunicativi con elevate caratteristiche di performance.

Peraltro, le nuove tecnologie 5G diventano abilitanti per ulteriori evoluzioni nella robotica e nella realtà aumentata.

L'**International Federation of Robotics**[2] nel *Rapporto World Robotics 2021* ha analizzato l'andamento del mercato della robotica nel 2020 prospettando un vertiginoso incremento delle vendite soprattutto in ambito sanitario. Analogamente si attende nel futuro una

[1] https://www.who.int/publications/i/item/9789240029200
[2] https://ifr.org/ifr-press-releases/news/service-robots-hit-double-digit-growth-worldwide

estensione delle applicazioni che fanno uso di tecnologie di Realtà aumentata anche attraverso le potenzialità dell'Internet of things.

Il Piano presente si pone in continuità con le versioni precedenti e con il Modello strategico di AgID adeguando le linee di azione ivi riportate alle mutate condizioni dello scenario normativo e tecnologico.

Sono riaffermati, di conseguenza, i principi base che recepiscono le linee di evoluzione già affermate con l'Agenda digitale europea che costituisce una delle sette iniziative faro della strategia "Europa 2020":

- Digital per default
- Cloud first
- Once only
- Speed only

Tutte le amministrazioni, comprese le aziende ospedaliere, sono tenute pertanto ad adeguare i propri piano di sviluppo ai principi su menzionati e a recepire le linee di indirizzo dettate dal Piano AgID.

Il principio "Digital per default" è il principio guida, esprimendo il concetto che ogni nuovo processo deve essere digitalizzato ("Full digital") e che, di conseguenza, ogni Amministrazione deve porre in essere gli interventi, anche graduali, necessari a digitalizzare tutti i processi di competenza.

La digitalizzazione deve peraltro essere condotta individuando soluzioni architetturali che prevedano, in prima analisi, il ricorso a piattaforme Cloud ("Cloud first"), utilizzando i dati già disponibili in altre amministrazioni ("Once only") e ricorrendo alla piattaforma Speed per l'autenticazione degli utenti ("Speed only").

Rispetto alle suindicate tematiche, gli IFO intendono progredire nel percorso di digitalizzazione e di innovazione avviando iniziative atte a:

- migliorare la relazione con gli assistiti attraverso il ricorso a strumenti/tecnologie che tendano ad aumentare la consapevolezza degli stessi nei percorsi di cura e ad abbattere le distanze con la struttura sanitaria e il suo personale
- migliorare le performance complessive degli Istituti attraverso una più incisa governance che riesca tramite la gestione ottimale del patrimonio informativo a ridurre le liste di attesa, ottimizzare l'uso dei posti letto, diminuire il tempo amministrativo di ogni medico a vantaggio del tempo di cura, incrementare l'efficacia chirurgica con l'ausilio della robotica e di altre innovazioni

A tal fine sarà necessario individuare ex ante i KPI quali-quantitativi che dovranno essere monitorati costantemente per individuare con la dovuta tempestività le azioni correttive che eventualmente dovranno attuarsi.

Obiettivi e spesa complessiva prevista

I principali obiettivi di digitalizzazione del triennio sono i seguenti:

- **Migrazione al Cloud delle componenti tecnologiche operanti in ambito di rete locale degli IFO** e inserite nel Piano di Migrazione predisposto anche in base alle indicazioni fornite dalla Regione Lazio con comunicazione prot. nr. 505366 del 10 maggio 2023 (anni 2023 – 2025);
- **Nuova Governance in Cloud del sistema informativo ospedaliero** (anni 2024 – 2026);
- **Potenziamento dell'infrastruttura in fibra ottica per i collegamenti dorsali e di piano** (anni 2023 – 2026);
- **Estensione della Piattaforma di workflow management finalizzata alla digitalizzazione dei consensi informati e del consenso informato privacy** presso tutti i reparti ed ambulatori degli IFO (anni 2023 – 2026);
- **Integrazione della Piattaforma di workflow management finalizzata alla digitalizzazione dei consensi informati e del consenso informato privacy** al fine di costituire la cartella clinica di reparto dell'assistito (anni 2023 – 2026);
- **Avvio ed estensione del sistema di indoor navigator** per guidare il paziente e gli eventuali accompagnatori all'interno delle strutture degli IFO (anni 2023 – 2026);

- **Evoluzione del sistema di conservazione digitale a norma** sia in ambito sanitario sia in ambito amministrativo (anni 2024 – 2026);
- **Evoluzione del sistema di sottoscrizione digitale a norma** sia in ambito sanitario sia in ambito amministrativo (anni 2024 – 2026);
- **Alimentazione del fascicolo sanitario elettronico 2.0** attraverso l'interfacciamento dei sistemi operanti in IFO (anni 2024 – 2026);
- **Evoluzione del sistema di business intelligence del sistema informativo ospedaliero** (anni 2023 – 2026);
- **Potenziamento ed evoluzione del sistema di sicurezza informatica ed implementazione della SOC** (anni 2023 – 2026);
- **Evoluzione del sistema amministrativo-contabile** (anni 2023 – 2026)**;**
- **Evoluzione del sistema di gestione delle risorse umane** (anni 2023 – 2026)**;**
- **Evoluzione del sistema di gestione degli atti e del protocollo informatico** (anni 2023 – 2026)**;**
- **Ammodernamento del parco tecnologico ospedaliero** da effettuarsi anche con il ricorso alle risorse PNRR (anni 2023 – 2026);
- **Evoluzione del Portale aziendale** attraverso manutenzione del sito internet e implementazione di una soluzione in grado di gestire e veicolare internamente il flusso delle informazioni organizzandole secondo logiche collaborative permettendo una più sicura connessione dall'esterno della rete aziendale (anni 2023 – 2026);
- **Evoluzione della Piattaforma di telemedicina, televisita e telemonitoraggio per l'attivazione di servizi di assistenza continua verso gli assistiti**
- **Evoluzione del sistema informativo ospedaliero**

PARTE IIa – LE COMPONENTI TECNOLOGICHEE I TEMI PROGETTUALI

Di seguito si descrivono i principali interventi sulle componenti amministrative del sistema informatico e per il potenziamento infrastrutturale ricompresi come componenti tecnologiche e i Temi Progettuali che riguardano le tematiche della Sanità Digitale.

Corrispondenza Obiettivi Componente tecnologica/progetti

Obiettivo		Componente Tecnologica/Progetto	Fondi
1	**Migrazione al Cloud**	Componente Tecnologica 1	PNRR
2	**Nuova Governance in Cloud**	Componente Tecnologica 1	PNRR + Regionali
3	**Potenziamento infrastruttura in f.o.**	Componente Tecnologica 2	Regionali
4	**Estensione della Piattaforma dei Consensi**	Tema Progettuale 1	Regionali
5	**Integrazione della Piattaforma dei Consensi**	Tema Progettuale 1	Regionali
6	**Indoor navigator**	Tema Progettuale 1	Regionali
7	**Evoluzione del sistema di conservazione**	Componente Tecnologica 2	Regionali
8	**Evoluzione del sistema di sottoscrizione**	Componente Tecnologica 2	Regionali
9	**Alimentazione del fascicolo sanitario elettronico 2.0**	Tema Progettuale 2	PNRR
10	**Evoluzione del sistema di business intelligence sanitario**	Tema Progettuale 3	Regionali
11	**Potenziamento ed evoluzione del SGSI e SOC**	Componente Tecnologica 4	Regionali
12	**Evoluzione del sistema amministrativo-contabile**	Componente Tecnologica 2	Regionali
13	**Evoluzione del sistema di gestione delle RU**	Componente Tecnologica 2	Regionali
14	**Evoluzione del sistema di gestione degli atti**	Componente Tecnologica 2	Regionali
15	**Ammodernamento del parco tecnologico**	Componente Tecnologica 2	PNRR + Regionali
16	**Evoluzione del Portale aziendale**	Componente Tecnologica 2	Regionali
17	**Evoluzione Piattaforma di telemedicina, televisita e telemonitoraggio**	Tema Progettuale 3	PNRR + Regionali
18	**Evoluzione del sistema informativo ospedaliero**	Tema Progettuale 3	Regionali

Principali riferimenti normativi italiani:

- Legge 9 gennaio 2004, n. 4 - Disposizioni per favorire e semplificare l'accesso degli utenti e, in particolare, delle persone con disabilità agli strumenti informatici
- Decreto legislativo 7 marzo 2005, n. 82 - Codice dell'amministrazione digitale (in breve CAD), art. 7, 68, 69 e 71
- Decreto Legislativo 10 agosto 2018, n. 106 - Attuazione della direttiva (UE) 2016/2102 relativa all'accessibilità dei siti web e delle applicazioni mobili degli enti pubblici
- Decreto Legge 18 ottobre 2012, n. 179 - Ulteriori misure urgenti per la crescita del Paese, art. 9, comma 7
- Linee Guida AGID per il design dei servizi digitali della Pubblica Amministrazione
- Linee Guida AGID sull'accessibilità degli strumenti informatici
- Linee Guida AGID sull'acquisizione e il riuso del software per la Pubblica Amministrazione

Principali riferimenti normativi europei:

- Regolamento (UE) 2018/1724 del Parlamento Europeo e del Consiglio del 2 ottobre 2018 che istituisce uno sportello digitale unico per l'accesso a informazioni, procedure e servizi di assistenza e di risoluzione dei problemi e che modifica il regolamento (UE)
- Direttiva UE 2016/2102 del Parlamento Europeo e del Consiglio del 26 ottobre 2016 relativa all'accessibilità dei siti web e delle applicazioni mobili degli enti pubblici

CAPITOLO 1. Componente Tecnologica 1 “Migrazione al Cloud”

La Strategia Cloud Italia, realizzata dal Dipartimento per la trasformazione digitale e dall'Agenzia per la cybersicurezza nazionale (ACN), contiene gli indirizzi strategici per il percorso di migrazione verso il cloud di dati e servizi digitali della Pubblica Amministrazione. Il documento illustra i criteri di classificazione di dati e servizi e la composizione della infrastruttura ad alta affidabilità (Polo Strategico Nazionale) che ospiterà i servizi strategici e critici.

La strategia risponde a tre sfide principali: assicurare l’autonomia tecnologica del Paese, garantire il controllo sui dati e aumentare la resilienza dei servizi digitali. In coerenza con gli obiettivi del Piano Nazionale di Ripresa e Resilienza, il documento traccia un percorso definito per accompagnare circa il 75% delle PA italiane nella migrazione dei dati e degli applicativi informatici verso un ambiente cloud.

Contesto normativo e strategico

Riferimenti normativi italiani:

- Circolare AGID n.2/2018, Criteri per la qualificazione dei Cloud Service Provider per la Pubblica Amministrazione
- Circolare Agenzia per l’Italia Digitale n.3/2018, Criteri per la qualificazione di servizi SaaS per il Cloud della Pubblica Amministrazione
- Strategia Cloud Italia
- Regolamento Cloud pubblicato il 15 dicembre 2021 con Determinazione AgID 628/2021
- Determina ACN n. 306 del 18 gennaio 2022
- Determina ACN n. 307 del 18 gennaio 2022
- Decreto direttoriale ACN n. 29 del 2 gennaio 2023

Costi attesi (Iva inclusa)

Attività	Contratti di forniture/servizi	Anno 2023	Anno 2024	Anno 2025
[01-01]	Decreto n. 48 – 3/2023 – PNRR per il finanziamento agli IFO per la migrazione al Cloud a valere sull'investimento 1.1	0,00	688.953,00	0,00
	Determina IFO n. 683/2023 Servizio Specialistico per la Progettazione	22.875,00	22.875,00	

Obiettivi e risultati attesi

- Migrare i workload applicativi attualmente operanti nella rete locale degli IFO in ambiente Cloud utilizzando le soluzioni offerte dal Polo Strategico Nazionale
- Avviare gli interventi in linea con la strategia unitaria regionale individuata dalla Cabina di Regia per assicurare la coerenza tra gli interventi e il coordinamento dei progetti
- Garantire opportuna protezione ai dati e ai servizi critici e ordinari a infrastrutture e servizi cloud che li trattano, in relazione ai livelli minimi e alle caratteristiche che devono assicurare le infrastrutture digitali e i servizi Cloud

- Risultati attesi

1 Incremento del livello di adozione del programma di abilitazione al cloud

1.1 Baseline 2023 – Numero dei servizi da migrare in Cloud
1.2 Target 2024 – Migrazione dei servizi in Cloud
1.3 Target 2025 – Avviare nuovo processo di Governance del sistema

Cosa deve fare l'Amministrazione

- **Migrazione al Cloud [codice 01-01]**
  - Implementare il Piano di Migrazione di seguito riportato
  - Scelta della modalità per il move dei workload da vm on premise all'infrastruttura private IAAS (HA)
  - Acquisizione dei servizi per l'utilizzo di Blade
  - Valutazione dei Blade da acquisire in base a Core e RAM di ogni istanza da migrare
  - Definire per ogni istanza gli elementi aggiuntivi da prevedere per la sicurezza
  - Calcolare il potenziale costo di migrazione

- Eventuali azioni di correzione da attuare per rendere sostenibile il modello

Servizio dell'amministrazione	Tipo di migrazione
ASSISTENZA FARMACEUTICA	Modalità A - Trasferimento in sicurezza dell'infrastruttura IT
PERCORSI ASSISTENZIALI INTEGRATI	Modalità A - Trasferimento in sicurezza dell'infrastruttura IT
CURE DOMICILIARI (ANCHE PALLIATIVE)	Modalità A - Trasferimento in sicurezza dell'infrastruttura IT
RICOVERO ORDINARIO PER ACUTI	Modalità A - Trasferimento in sicurezza dell'infrastruttura IT
DAY SURGERY	Modalità A - Trasferimento in sicurezza dell'infrastruttura IT
DAY HOSPITAL	Modalità A - Trasferimento in sicurezza dell'infrastruttura IT
RIABILITAZIONE E LUNGODEGENZA POST ACUZIE	Modalità A - Trasferimento in sicurezza dell'infrastruttura IT
ATTIVITÀ TRASFUSIONALI	Modalità A - Trasferimento in sicurezza dell'infrastruttura IT
ATTIVITÀ DI TRAPIANTO DI CELLULE, ORGANI E TESSUTI	Modalità A - Trasferimento in sicurezza dell'infrastruttura IT
ATTIVITÀ DIAGNOSTICA	Modalità A - Trasferimento in sicurezza dell'infrastruttura IT
ASSISTENZA SPECIALISTICA AMBULATORIALE	Modalità A - Trasferimento in sicurezza dell'infrastruttura IT
GESTIONE MALATTIE INFETTIVE E PARASSITARIE (INCLUSI PROGRAMMI VACCINALI)	Modalità A - Trasferimento in sicurezza dell'infrastruttura IT
SORVEGLIANZA, PREVENZIONE E TUTELA DELLA SALUTE E SICUREZZA NEI LUOGHI DI LAVORO	Modalità A - Trasferimento in sicurezza dell'infrastruttura IT
GESTIONE DELLE MALATTIE CRONICHE, SCREENING E NUTRIZIONE	Modalità A - Trasferimento in sicurezza dell'infrastruttura IT
ATTIVITÀ MEDICO LEGALI PER FINALITÀ PUBBLICHE	Modalità A - Trasferimento in sicurezza dell'infrastruttura IT
ASSISTENZA A PARTICOLARI CATEGORIE	
	Modalità A - Trasferimento in sicurezza dell'infrastruttura IT
RETI DI PATOLOGIA	Modalità A - Trasferimento in sicurezza dell'infrastruttura IT
RISCHIO CLINICO	Modalità A - Trasferimento in sicurezza dell'infrastruttura IT
EDUCAZIONE CONTINUA IN MEDICINA	Modalità A - Trasferimento in sicurezza dell'infrastruttura IT
ANAGRAFE NAZIONALE ASSISTIBILI	Modalità A - Trasferimento in sicurezza dell'infrastruttura IT
FASCICOLO SANITARIO REGIONALE	Modalità A - Trasferimento in sicurezza dell'infrastruttura IT
RAPPORTI CON L'UTENZA - URP	Modalità A - Trasferimento in sicurezza dell'infrastruttura IT
COMUNICAZIONE ISTITUZIONALE WEB E OPEN DATA	Modalità A - Trasferimento in sicurezza dell'infrastruttura IT
PROTOCOLLO	Modalità A - Trasferimento in sicurezza dell'infrastruttura IT
GESTIONE DOCUMENTALE	Modalità A - Trasferimento in sicurezza dell'infrastruttura IT
CONSERVAZIONE DIGITALE	Modalità A - Trasferimento in sicurezza dell'infrastruttura IT
PERSONALE	Modalità A - Trasferimento in sicurezza dell'infrastruttura IT
CONTABILITÀ, BILANCIO E CONTROLLO	Modalità A - Trasferimento in sicurezza dell'infrastruttura IT
ACQUISTI	Modalità A - Trasferimento in sicurezza dell'infrastruttura IT
PRODUTTIVITÀ INDIVIDUALE E COLLABORATION	Modalità A - Trasferimento in sicurezza dell'infrastruttura IT

Il piano di migrazione sopra riportato è stato generato automaticamente estraendolo dalla candidatura n.84998 inviata in data 22/05/2023 tramite la piattaforma PA Digitale 2026, in adesione all'avviso 1.1 e 1.2 "Infrastrutture digitali e abilitazione al cloud" - ASL/AO -marzo 2023 del 14/03/2023.

CAPITOLO 2. Componente tecnologica 2 "Potenziamento infrastrutturale ed architetturale"

La sostenibilità delle azioni di digitalizzazione degli Istituti non può prescindere dal rafforzamento delle Tecnologie della Comunicazione e dell'Informazione al fine di assicurare un adeguato livello di sicurezza informatica e della qualità dell'offerta di assistenza e di cura, dell'efficienza e dell'efficacia dei processi di front e di back office e di un'evoluzione in linea con il mutamento dei fabbisogni correlati al Piano di Migrazione al Cloud.

Contesto normativo e strategico

Riferimenti normativi italiani:

- Linee Guida AGID per il design dei servizi digitali della Pubblica Amministrazione
- Linee Guida AGID sull'accessibilità degli strumenti informatici
- Linee Guida AGID sull'acquisizione e il riuso del software per la Pubblica Amministrazione
- Determinazioni ACN

Riferimenti normativi europei: Non applicabile

Costi attesi (Iva inclusa)

Attività	Contratti di forniture/servizi	Anno 2023	Anno 2024	Anno 2025
[02-01]	Determina n. 471/2023 Adesione Convenzione Consip "PERSONAL COMPUTER DESKTOP ULTRACOMPATTI LOTTO 1	50.855,70	0,00	0,00
	Determina n. 382/2023 Acquisto Portale Intranet	48.531,60		
	Determina n. 728/2023 Personalizzazione Portale Intranet	28.609,00	0,00	0,00
	Determina n. 470/2023 Lettori di timbraturre	8.283,80	2.196,00	2.196,00
	Determina n. 856/2023 Acquisto Tablet	24.339,00		
	Determina n. 805/2023 Licenze varie	4.453,00		

	Determina n. 740/2023 Licenze SAAS	14.518,00	29.036,00	
	Determina n. 371/2023 Adesione Convenzione Consip "telefonia fissa 5"	217.616,97		
[02-02]	Determina n. 705/2023 Mobile Threat Defense	10.917,78		
	Determina n. 385/2023 Cyber Defence	43.810,20		

Obiettivi e risultati attesi

- Migliorare la dotazione IT degli Istituti attraverso il ricorso alle Convenzioni CONSIP e/o a procedure del Mercato Elettronico della Pubblica Amministrazione (MEPA)
- Ampliare le tipologie di documenti da prevedere in conservazione digitale a norma
- Evolvere le funzionalità del sistema per la gestione del workflow per la formazione e la definizione delle deliberazioni e delle determinazioni
- Aggiornare il Portale istituzionale per migliorarne la fruibilità e la navigazione tra contenuti
- Migliorare la diffusione di soluzioni di firma digitale in remoto
- Incrementare la sicurezza del SGSI attraverso il ricorso a soluzioni di tipo SOC e di analisi mirato ed evoluto degli eventi al fine di prevenire intrusioni, esfiltrazioni e comportamenti non in linea con le policy aziendali

- Risultati attesi

Diffusione del modello di riuso di software tra le amministrazioni in attuazione delle Linee Guida AGID sull'acquisizione e il riuso del software per la Pubblica Amministrazione

  - Baseline 2023 - Individuazione numero di software open source rilasciati
  - Target 2024 - Incremento numerico dei software open point pari a +1 rispetto alla Baseline
  - Target 2025 - Incremento numerico dei software open point pari a +2 rispetto alla Baseline

Cosa deve fare l'Amministrazione

- **Potenziamento Asset [codice 02-01]**

  - Acquisizione di personal computer in relazione al numero di apparecchiature da porre in stato di obsolescenza
  - Acquisizione di personal computer del tipo "Portatili" e Tablet in relazione alle esigenze manifestate dal Personale amministrativo, sanitario, di ricerca
  - Gestione del parco apparecchiature in uso
  - Aggiornamento licenze
  - Verifica di potenziali software in riuso/open source di interesse per gli Istituti
  - Manutenzione sito istituzionale
  - Implementazione del Portale della nuova Intranet
  - Realizzazione nuove dorsali di fibra ottica

- **Evoluzione del SGSI ed implementazione di un sistema SOC [codice 02-02]**

Anche in ambito sanitario, come quello finanziario e di security, sta assumendo sempre più rilevanza la necessità di attuare misure organizzative e tecnologiche adeguate a mitigare i rischi derivanti da attacchi informatici.

Il contesto internazionale propone sempre con maggiore frequenza attacchi cibernetici mirati a interrompere l'erogazione di servizi essenziali o ad entrare in possesso dei dati personali/sensibili dei cittadini, soprattutto in considerazione delle note vicende belliche.

Per far fronte alla crescente minaccia occorre attuare iniziative che consolidino la sicurezza del sistema informatico degli IFO e consentano di assicurare un adeguato livello di protezione dei dati e delle apparecchiature sanitarie.

In linea con quanto previsto dal quadro normativo nazionale (Piano triennale dell'informatica nella Pubblica amministrazione, Quadro strategico nazionale per la sicurezza dello spazio cibernetico, Direttiva Nis, …) è stato ideato il framework di riferimento che, ispirato al Cybersecurity Framework del NIST (National Institute of Standards and Technology),

costituisce lo strumento operativo di riferimento per organizzare il Sistema di gestione della sicurezza (SGSI) all'interno dell'Azienda.

- Implementare processi di rilevamento di defect, bug e flaw
- Implementare automatismi di monitoraggio e segnalazione efficaci
- Implementare meccanismi di classificazione in base alla facilità di exploit
- Organizzare un Team per costituire un Network Operation Center come struttura orientata alla gestione da remoto di problematiche di networking e infrastruttura, operativo 24 su 24, 7 su 7 con i seguenti obiettivi:
    - Supervisione delle attività sistemistiche
    - Monitoraggio puntuale e tracciamento delle attività
    - Controllo sulle attività di gestione networking, dispositivi e accessi

IFO, inoltre, si pone l'obiettivo di implementare un Security Operations Center (SOC) che rappresenta ormai il cuore pulsante della difesa cibernetica di un'organizzazione. È un centro operativo in cui vengono monitorati, analizzati e risposto ai possibili attacchi informatici in tempo reale. Il SOC si avvale di strumenti avanzati, come sistemi di rilevamento delle minacce, analisi comportamentale, e intelligence sulle minacce, per identificare e contrastare le intrusioni nei sistemi informatici.

Nei contesti delle aziende sanitarie pubbliche, un SOC è vitale per mantenere la sicurezza dei dati sensibili dei pazienti e dei sistemi medici. Può proteggere contro attacchi come ransomware, che potrebbero paralizzare le operazioni cliniche. Il SOC monitora costantemente le reti e i dispositivi medici per individuare comportamenti sospetti o intrusioni. Attraverso l'analisi in tempo reale dei dati, può prevenire e mitigare attacchi, riducendo il rischio di interruzioni delle attività cliniche e garantendo la continuità delle cure ai pazienti. Inoltre, fornisce una risposta rapida e efficace in caso di violazioni, limitando i danni e ripristinando la sicurezza dei sistemi.

CAPITOLO 3. Componente Tecnologica 3 “Gestione dei flussi documentali”

Le nuove Linee Guida AgID sul documento informatico, entrate in vigore il 1 gennaio 2022, hanno contribuito a rafforzare ed omogenizzare il quadro normativo di riferimento per la produzione, gestione e conservazione dei documenti informatici.

Contesto normativo e strategico

Riferimenti normativi italiani:

- Linee Guida Agid sulla formazione, gestione e conservazione dei documenti informatici (Determinazione n. 455/2021)

Riferimenti normativi europei: non applicabile

Costi attesi (Iva inclusa)

Attività	Contratti di forniture/servizi	Anno 2023	Anno 2024	Anno 2025
[03-02]	Determina n. 19/2023 per sistema Amministrativo-contabile	95.117,02		

Obiettivi e risultati attesi

- Evolvere ed aggiornare “Fascicoli Digitali” per conseguire una più efficace ricerca di atti e documenti
- Valutazioni sull’adozione del sigillo elettronico per incrementare il livello di integrità del documento
- Digitalizzazione di specifici processi attraverso il ricorso a funzioni di workflow management
- Aggiornamento del manuale di conservazione degli atti

Cosa deve fare l’Amministrazione

- **Gestione delle determine/delibere aziendali e del protocollo informatico [codice 03-01]**

La loro applicazione integrale richiede un impegno costante ed oneroso in termini di azioni interne per rendere effettivi e consolidati le novità introdotte.

Gli aspetti più importanti sui quali IFO dovrà impegnarsi riguardano:

- Metadati
- segnatura di protocollo
- interoperabilità Gruppo
- Conservazione di basi di dati Gruppo
- Interoperabilità tra erogatori di servizi di conservazione

- **Piattaforma Amministrativo-contabile [codice 03-02]**

Con convenzione stipulata tra gli IFO e la ASL di Viterbo in data 10 maggio 2021 hanno stipulato specifico accordo per la cessione in riuso del sistema denominato SISAR AMC che dovrà essere oggetto di servizi di personalizzazione in relazione alle indicazioni che perverranno dalle strutture referenti (ABS, Farmacia, …) anche in relazione ai flussi informativi da trasmettere alla Regione Lazio.

- **Piattaforma Risorse Umane [codice 03-03]**

La *Digital Transformation* ha impatti anche con l'organizzazione di un'Azienda Ospedaliera ed è stimolo per avviare nuovi modelli di gestione delle Risorse Umane che servono a definire competenze, strumenti e processi in continuo allineamento con le nuove organizzazioni e modalità di lavoro.

Il personale rappresenta un fattore strategico di successo per l'Azienda che è dunque chiamata a focalizzarsi sulla crescita professionale e motivazionale.

I principali obiettivi si concretizzano in:

- Modello di competenze
- Fascicolo del dipendente
- Sistemi di rilevazioni presenze
- Gestioni paperless

CAPITOLO 4. Tema Progettuale 1 “Patient journey”

La nuova visione delle Organizzazioni sanitarie si incentra sul concetto di *Patient Journey* ossia sull’affermazione di un paradigma organizzativo che va oltre il semplice concetto di centralizzazione del paziente, ma che individua il paziente come un soggetto proattivo nel ridisegno dei processi sanitari.

Non è solo una questione di condivisione, ma è l’affermazione suprema del concetto di Patient Engagement che si concretizza in una visione che va oltre il semplice rapporto con l’Organizzazione sanitaria ma che ricomprende un percorso completo che va dall’Accettazione all’eventuale Prestazione Chirurgica e alle terapie postoperatorie e trova la sua sublimazione nel rapporto con il Paziente cronico.

La digitalizzazione può costituire una delle leve principali per la realizzazione del nuovo modello organizzativo, consentendo peraltro di consentire al paziente di avere la massima consapevolezza del percorso di cura.

Contesto normativo e strategico

Riferimenti normativi italiani:

- Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 “Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali”
- Provvedimento generale prescrittivo in tema di biometria del 12 novembre 2014
- Linee guida per la Dematerializzazione del Consenso Informato in ambito radiologico emanate dall’Agenzia per l’Italia digitale 6. Decreto legislativo 30 giugno 2003, n. 196 e s.m.i.
- Decreto legislativo 7 marzo 2005, n. 82 (Codice dell’Amministrazione Digitale) e s.m.i.
- Legge 22 dicembre 2017, n. 219 “Norme in materia di consenso informato e di disposizioni anticipate di trattamento”
- Documento di indirizzo sul consenso informato adottato con Determinazione 25 gennaio 2022, n. G00642 dalla Direzione Salute e Integrazione Sociosanitaria della Regione Lazio (di seguito Documento di Indirizzo)

Riferimenti normativi europei:

- Regolamento europeo n. 910/2014

Costi (Iva inclusa)

Attività	Contratti di forniture/servizi	Anno 2023	Anno 2024	Anno 2025
[04-01]	Delibera IFO n. 383/2023	51.118,00	0,00	0,00
[04-02]	Delibera IFO n. 504/2022	38.430,00		
[04-03]	Delibera IFO n. 241/2023	152.500,00	0,00	0,00

Obiettivi e risultati attesi

- Incrementare la soddisfazione dell'assistito
- Progettare percorsi di cura personalizzati
- Affiancarsi all'assistito in fase pre/post operatoria
- Passare dal concetto di curare a quello del prendersi cura
- Progettare nuovi metodi di terapie e di cura remotizzati "in house"

Cosa deve fare l'Amministrazione

- **Consenso Informato [codice 04-01]**

Il progetto di acquisizione e di gestione del consenso informato in modalità digitale si colloca nell'ambito del processo di graduale dematerializzazione dei documenti clinici e sanitari avviato dagli Istituti negli ultimi anni.

In particolare, il progetto prevede l'utilizzo di una Piattaforma che consente l'acquisizione del consenso del paziente alla prestazione sanitaria mediante sottoscrizione della firma grafometrica per mezzo di un tablet.

La piattaforma gestisce l'intero processo di firma prevedendo anche la fase prodromica di erogazione dell'informativa e di eventuali contributi multimediali, audiovisivi ed infografici erogabili per migliorare la comprensione del paziente e renderlo quanto più possibile consapevole del trattamento sanitario che è proposto dall'equipe medica.

E' prevista è la possibilità di verificare il grado di reale apprendimento dell'assistito tramite una batteria di test inserendo specifiche domande sui rischi connessi allo specifico trattamento. In questo caso, la sottoscrizione del consenso è consentita solo ed esclusivamente nei casi in cui il paziente risponda correttamente ai test e, in caso di risposte sbagliate, ripropone le sezioni relative agli errori commessi.

La firma grafometrica prevista in CONFIRMO consente di acquisire le manifestazioni di volontà degli assistiti in conformità alla normativa vigente con particolare riferimento al decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 recante "Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali". I documenti informatici sottoscritti con FEA grafometrica, a norma di legge, costituiscono dei documenti nativi digitali e sono da conservare conformemente alla normativa vigente.

L'assistito può richiedere in ogni momento di accedere ai consensi prestati così come può anche richiedere il recesso.

Il piano graduale di estensione prevede una fase pilota avviata nel 2023 ed unafase graduale di estensione entro il 2024, prevedendo le attività per integrare la piattaforma con i sistemi di cartella clinica in modo che il Consenso, dopo la sottoscrizione, sia inserito automaticamente nella Cartella Clinica digitale del paziente.

MATRICE RESPONSABILITA'

1^ opzione

Ruolo / Attività		Primario/ Responsabile Struttura	Medici	Altro Personale sanitario	Personale Amministrativo	Direzione Medica	UOSD Informatica	Assistito	Settore Privacy	Fornitore
1	Anagrafica Assistiti	NOT APPLICABLE	NOT APPLICABLE	NOT APPLICABLE	NOT APPLICABLE	NOT APPLICABLE	NOT APPLICABLE	NOT APPLICABLE	NOT APPLICABLE	NOT APPLICABLE
2	Anagrafica Medici	(1)Fornisce elenco a UOSD Informatica	NOT APPLICABLE	NOT APPLICABLE	NOT APPLICABLE	NOT APPLICABLE	(2)Inserisce nominative	NOT APPLICABLE	NOT APPLICABLE	NOT APPLICABLE
3	Anagrafica altro Personale	(1)Fornisce elenco a UOSD Informatica	NOT APPLICABLE	NOT APPLICABLE	NOT APPLICABLE	NOT APPLICABLE	(2)Inserisce nominativi	NOT APPLICABLE	NOT APPLICABLE	NOT APPLICABLE
4	Supporto Procedurale	(3)Coordina le attività da porre in essere e monitora l'esatto adempimento	(4) Assicura l'esatto adempimento	(4) Assicura l'esatto adempimento	NOT APPLICABLE	(2)Dirama le istruzioni procedurali	(1)Predispone le istruzioni di competenza	NOT APPLICABLE	NOT APPLICABLE	NOT APPLICABLE
5	Assistenza Tecnica	NOT APPLICABLE	NOT APPLICABLE	(1)Richiede Assistenza operative/applicativa	(1)Richiede Assistenza operative/applicativa	NOT APPLICABLE	(2)Fornisce Assistenza per problematiche su Tablet, wifi e infrastruttura	NOT APPLICABLE	NOT APPLICABLE	(2)Fornisce Assistenza per problematiche applicative
6	Pubblicazione sito Internet	NOT APPLICABLE	NOT APPLICABLE	NOT APPLICABLE	NOT APPLICABLE	(1)Fornisce a UOSD Informatica modelli da pubblicare e informazioni da diffondere	(2)Richiede la pubblicazione sul sito delle informative e dei consensi oltre che delle altre informazioni per accesso e recesso	NOT APPLICABLE	NOT APPLICABLE	NOT APPLICABLE
7	Tablet	(2)Designa referente per custodia	NOT APPLICABLE	(3)Chi designato come custode provvede a organizzare la disponibilità del tablet la mattina e la consegna a fine giornata	NOT APPLICABLE	NOT APPLICABLE	(1)Fornisce i tablet	NOT APPLICABLE	NOT APPLICABLE	NOT APPLICABLE
8	Trattamento dei dati	Responsabile del trattamento	Incaricato	Incaricato	Incaricato	NOT APPLICABLE	Incaricato	NOT APPLICABLE	Rapporti con il DPO	Responsabile esterno
9	Informativa Orale	NOT APPLICABLE	NOT APPLICABLE	(Fase Pilota) Informa il paziente	(A regime) Informa il paziente	NOT APPLICABLE	NOT APPLICABLE	E' informato della possibilità di ricorrere alla firma grafometrica per la sottoscrizione del consenso	NOT APPLICABLE	NOT APPLICABLE
10	Identificazione Assistiti	NOT APPLICABLE	NOT APPLICABLE	(Fase Pilota) Identifica l'Assistito	(A regime) Identifica l'Assistito	NOT APPLICABLE	NOT APPLICABLE	(2)Fornisce a richiesta dati anagrafici e copia documento di riconoscimento	NOT APPLICABLE	NOT APPLICABLE
11	Consenso Generale alle cure	(3) Monitoraggio attività	NOT APPLICABLE	(4)Supporta l'Assistito	NOT APPLICABLE	(1)Definisce il modello di riferimento	(2)Configura Piattaforma CONFIRMO	NOT APPLICABLE	NOT APPLICABLE	NOT APPLICABLE
12	Informative	(3) Monitoraggio attività	NOT APPLICABLE	(4)Supporta l'Assistito	NOT APPLICABLE	(1)Definisce il modello di riferimento	(2)Configura Piattaforma CONFIRMO	NOT APPLICABLE	NOT APPLICABLE	NOT APPLICABLE

13	Consenso specifico al trattamento sanitario	(3) Monitoraggio attività	NOT APPLICABLE	(4)Supporta l'Assistito	NOT APPLICABLE	(1)Definisce il modello di riferimento	(2)Configura Piattaforma CONFIRMO	NOT APPLICABLE	NOT APPLICABLE	NOT APPLICABLE
14	Acquisizione copia f/r del documento di riconoscimento	NOT APPLICABLE	NOT APPLICABLE	(Fase Pilota) (1) Acquisisce copia fronte retro	Fase Pilota) (1) Acquisisce copia fronte retro	NOT APPLICABLE	NOT APPLICABLE	NOT APPLICABLE	NOT APPLICABLE	NOT APPLICABLE
15	Informativa FEA	NOT APPLICABLE	NOT APPLICABLE	(Fase Pilota) Supporta il paziente	(A regime) Supporta il paziente	NOT APPLICABLE	NOT APPLICABLE	NOT APPLICABLE	NOT APPLICABLE	NOT APPLICABLE
16	Consenso FEA	NOT APPLICABLE	NOT APPLICABLE	(Fase Pilota) Supporta il paziente	(A regime) Supporta il paziente	NOT APPLICABLE	NOT APPLICABLE	NOT APPLICABLE	NOT APPLICABLE	NOT APPLICABLE
17	Informativa Privacy	NOT APPLICABLE	NOT APPLICABLE	(Fase Pilota) (3)Supporta il paziente	(A regime) (3)Supporta il paziente	NOT APPLICABLE	NOT APPLICABLE	(2)Compila modello	(1)Definisce il modello di riferimento	NOT APPLICABLE
18	Richiesta di Recesso	(3)Coordina il riscontro individuando la persona che dà seguito alla richiesta	NOT APPLICABLE	(4)La persona individuate che dà seguito alla richiesta	NOT APPLICABLE	(2)Riceve la richiesta di accesso e la gestisce indirizzandola alla struttura competente e gestendo il riscontro	NOT APPLICABLE	(1) Trasmette la richiesta di recesso	NOT APPLICABLE	NOT APPLICABLE
19	Richiesta di Accesso	(3)Coordina il riscontro individuando la persona che dà seguito alla richiesta	NOT APPLICABLE	(4)La persona individuate che dà seguito alla richiesta	NOT APPLICABLE	(2)Riceve la richiesta di accesso e la gestisce indirizzandola alla struttura competente e gestendo il riscontro	NOT APPLICABLE	(1) Trasmette la richiesta di accesso	NOT APPLICABLE	NOT APPLICABLE

- **Navigazione Indoor [codice 04-02]**

Per gli assistiti, muoversi tra i reparti e gli ambulatori di un'azienda ospedaliera non è mai semplice, in considerazione dell'ampiezza degli spazi e dell'allocazione deframmentata delle varie strutture.

Per semplificare gli spostamenti, soprattutto delle persone con difficoltà motorie, si è avviato un progetto che ricorre alla tecnologia per guidare l'assistito a raggiungere la destinazione desiderata nel modo più semplice possibile.

La piattaforma sfrutta difatti i punti di accesso wireless Wi-Fi per fornire una posizione precisa della persona.

La navigazione indoor e il posizionamento indoor aiutano gli assistiti a identificare dove si trova il punto di destinazione e il relativo percorso da seguire per raggiungerlo dalla posizione di partenza, attraverso il rilevamento automatico della posizione e algoritmi di IA che aiutano la persona ad arrivare alla meta migliorando le pratiche di sicurezza e protezione.

Il Progetto è in fase di avvio e si stima di concludere le attività entro il 2024

- **Gestione delle file di attesa degli ambulatori [codice 04-03]**

Tra le mission degli IFO vi è la centralità del paziente, è intenzione di questi Istituti agevolare il più possibile gli utenti per la fruizione delle prestazioni, evitando file e conseguenti assembramenti ed al contempo semplificare il *patient journey* attraverso sistemi digitali di ultima generazione customizzati e pensati in un'ottica di *operation management* al fine di ottimizzare la procedura di presa in carico.

IFO ha attivato un sistema intelligente in grado di gestire, presso le strutture oncologiche, le prenotazioni, gli arrivi, le assegnazioni paziente day hospital/ambulatorio, le richieste di esami diagnostici aggiuntivi, l'aggiornamento interattivo dell'agenda giornaliera e l'erogazione delle chemioterapie in funzione della disponibilità del farmaco chemioterapico.

Il software deve poter importare automaticamente i già menzionati dati dei pazienti secondo quanto schedulato in agenda, consentendo la gestione del corretto svolgimento delle attività. In particolare, il suindicato software giornalmente dovrà importare l'agenda (dal software di agenda di reparto formato VbA) creata dagli operatori di reparto, permettendo di gestire dal pannello amministrativo le tabelle delle varie terapie, i relativi tempi e la gestione delle stanze diversificate con differenti colori.

Inoltre, il software oltre a gestire la fila dei pazienti in attesa, dovrà registrare i tempi di attesa ed il numero di persone presenti e la reportistica associata.

- **Centrale Operativa Territoriale [codice 04-04]**

Nella "MISSIONE 6: SALUTE" ed in particolare alla Componente M6C1 con la dicitura "Reti di Prossimità, Strutture e Telemedicina per l'assistenza Sanitaria Territoriale" viene ripreso un concetto basilare della riforma Sanitaria della 833/78, cioè: L'assistenza alla persona deve rappresentare una attività continua, che si trasforma secondo il livello di intensità e di cronicità della malattia.

La Centrale Operativa Territoriale (COT) degli IFO si pone l'obiettivo di garantire la continuità assistenziale necessaria per il paziente oncologico e razionalizza l'utilizzo delle risorse nella fase di dimissione protetta dall'Ospedale verso il Territorio.

La peculiarità di patologie e pazienti afferenti agli IFO, sia nell'Istituto Regina Elena che nell'Istituto San Gallicano, richiedono una importante relazione con le strutture territoriali.

Per fare ciò è prevista la costruzione di una relazione organica tra la COT IFO e le COT aziendali delle ASL di residenza dei pazienti al fine di facilitare la precoce presa in carico delle persone in dimissione.

E' altresì necessario, per tracciare i percorsi dei pazienti, monitorare i processi interni per il cambio di setting ed integrare i MMG nei percorsi di cura delineati nei DMT con l'affidamento al MMG (o alle équipe territoriali) dei pazienti di IFO in cura cronica o in follow-up.

Obiettivi a breve termine:

a) rendere IFO un attore attivo della rete regionale

- gestire la logistica e i flussi dei pazienti in IFO, in entrata e in uscita attraverso la creazione di una Centrale di Continuità-COT, in collegamento con le COT-A e COT-D delle ASL di residenza dei pazienti.

b) potenziare la presa in carico longitudinale dei pazienti oncologici, dermatologici e con malattie rare. La Centrale di Continuità delle cure, nel ruolo di COT-IFO avrà il coordinamento delle funzioni di continuità assistenziale (Unità di valutazione multidimensionale, Sportelli di accesso, Case Manager) e transitional care per garantire al paziente il coordinamento generale delle attività che lo coinvolgono e l'affidamento strutturato in dimissione e in follow-up

CAPITOLO 5. Tema Progettuale 2 “Fascicolo sanitario elettronico 2.0”

L’11 luglio 2022 sono state pubblicate da AgID le Linee Guida di attuazione del Fascicolo Sanitario Elettronico (FSE), previste dal Decreto del 20 maggio 2022 emanato dal Ministero della Salute.

L’adozione delle Linee Guida è un tassello fondamentale per il raggiungimento degli obiettivi indicati dal PNRR: l’85% dei medici di base dovranno, infatti, alimentare il Fascicolo entro il 2025 e tutte le Regioni e Province Autonome dovranno adottare e utilizzare il Fascicolo entro il 2026.

Contesto normativo e strategico

Riferimenti normativi italiani:

- Decreto 20 maggio 2022 Ministero della Salute “Adozione delle Linee guida per l'attuazione del Fasciolo sanitario elettronico”
- Linee Guida AgID di attuazione del Fascicolo Sanitario Elettronico (FSE) dell’11 luglio 2022

Costi attesi (IVA Inclusa)

I costi sono calcolati all’interno dei contratti di affidamento dei servizi di evoluzione/manutenzione dei singoli sistemi gestionali.

Obiettivi e risultati attesi

All’interno della Missione 6, Componente 1 del Piano Nazionale di Ripresa e Resilienza (PNRR) rientra l’investimento 1.3.1 “Rafforzamento dell’infrastruttura tecnologica e degli strumenti per la raccolta, l’elaborazione, l’analisi dei dati e la simulazione” che prevede una specifica azione per il potenziamento del Fascicolo Sanitario Elettronico (FSE).

Gli obiettivi mirano a rendere il FSE il punto unico ed esclusivo di accesso per i cittadini ai servizi del SSN e uno strumento per le strutture sanitarie ed istituzioni sanitarie che possono utilizzare le informazioni raccolte dal FSE per l’analisi di dati clinici al fine di migliorare efficacemente l’offerta di servizi da erogare.

Cosa deve fare l'Amministrazione

Gli IFO, nell'ambito dell'iniziativa di coordinamento avviata dalla Regione, devono assicurare l'adeguamento dei propri sistemi in modo tale che i documenti prodotti possano essere indicizzati nel FSE secondo i nuovi standard nazionali.

La Regione metterà a disposizione delle Aziende Ospedaliere e delle Asl, di conseguenza anche per gli IFO, una Piattaforma di servizi di firma remota, a supporto del processo di produzione e firma dei documenti socio sanitari da indicizzare per l'alimentazione del FSE.

Cronoprogramma

AZIONE	INTERVENTO	2023	2024	2025	2026
Adeguamento componente centrale FSE, comprensiva degli elementi infrastrutturali a supporto	Progettazione ed adeguamento architettura				
	Consolidamento servizi di infrastruttura				
	Sviluppo sistemi di monitoraggio				
	Servizi di assistenza e manutenzione				
Evoluzione e implementazione dei nuovi servizi per gli assistiti da rendere fruibili, come da linee guida, attraverso il FSE	Adeguametno ed evoluzione dei servizi esistenti				
	Nuovi servizi ai cittadini				
	Nuovi servizi agli operatori				
	Servizi di assistenza e manutenzione				
Adeguamento sistemi aziendali produttori dei documenti da indicizzare nel FSE secondo i nuovi standard nazionali	Adeguamento sistemi dipartimentali strutture pubbliche				
	Adeguamento sistemi dipartimentali strutture private				
Servizi di supporto alla progettazione e alla gestione dell'iniziativa	Governance				

Documenti oggetti dell'intervento

Tipologia documento
LIS (Referto di laboratorio)
Cartella Ambulatoriale
Lettera di Dimissione Ospedaliera
Referto di Specialistica Ambulatoriale
RIS (Referto di Radiologia)
Anatomia Patologica

CAPITOLO 6. Tema Progettuale 3 “Clinical information system”

Si è, di recente, svolto a Porto il secondo simposio dell'Organizzazione mondiale della sanità (OMS) sul futuro della salute digitale in cui sono stati dibattuti differenti temi, dalle possibili minacce ed opportunità derivanti dal ricorso all'intelligenza artificiale (AI) alla necessità di riprogettare i servizi sanitari per incrementare la *governance* del patrimonio informativo (**Ecosistema dei dati sanitari**).

Gli esiti dell’evento e i vari report prodotti dall’OMS costituiscono una valida testimonianza delle opportunità offerte dalla tecnologia per migliorare i livelli di assistenza sanitaria sul territorio, in particolare lo studio approfondisce i benefici per supportare il management aziendale nelle fasi di *decision-making*, per ottimizzare la gestione dei farmaci, per migliorare il rapporto con il paziente e per promuovere la Telemedicina.

Partendo dal documento dell’OMS e da altri studi e ricerche disponibili in letteratura, gli IFO, in relazione anche allo stato di attuale di utilizzo delle tecnologie, hanno adottato un piano costante e di graduale miglioramento dei servizi che ricomprende l’aggiornamento dei dispositivi di ausilio all’attività sanitaria e l’implementazione di nuovi processi secondo gli approcci della *IA*, *big data*, *robotica* e *Mobile Health*.

Contesto normativo e strategico

Riferimenti normativi italiani: Non applicabile

Riferimenti normativi europei: Non applicabile

Costi attesi (IVA Inclusa)

Attività	Contratti di forniture/servizi	Anno 2023	Anno 2024	Anno 2025
[06-01]	Adesione Convenzione Consip	1.021.952,52	845.753,81	845.753,81
	Delibera IFO n. 159/2023 Servizio in SaaS di certificabilità e la tracciabilità del prodotto sterilizzato	42.273,00	6.039,00	
[06-02]	Delibera IFO n. 1190/2022	44.652,00		
[06-03]	Delibera IFO n. 669/2023	51.118,00	51.118,00	51.118,00

Obiettivi e risultati attesi

- Applicazione e diffusione del Paradigma del Connected Care
- Sensibilizzazione per l'utilizzo della User experience
- Incremento del numero di processi sanitari paperless
- Diffusione delle interconnessioni tra componenti interne del sistema informatico
- Valorizzazione dell'ecosistema dei dati sanitari
- Monitoraggio puntuale dei processi sanitari e loro performance

Cosa deve fare l'Amministrazione

- **Evoluzione del sistema di cartella clinica e delle componenti di interconnessione tra i vari sotto-sistemi [Codice 06-01]**

DESCRIZIONE FORNITURA	AVVIO
Area gestione Sale Operatorie: ORMAWEB	
Modulo gest. Interventi	2023
Canale di integrazione SIO (hl7/ws) - integrazione ADT	2023
LISTA Attesa Chirurgica	2023
Licenza SPECIALITA' CHIRURGICA (n° 11 reparti)	2023
Canale di integrazione SIO (via ws o hl7) - Integrazione MPI	2023
Gestione Magazzino Sala Operatoria	2023
Canale di integrazione SIO (hl7/ws) - integrazione Anatomia Patologica	2023
Visita Anestesiologica preoperatoria	2023
Cartella Anestesiologica informatizzata - Intraoperatoria	2023
Modulo gestione rischio clinico mediante checklist	2023
Laboratorio	
Sistema DNLAB	2023
Sistema EOS	2023
Sistema Prometeo Appropriatezza	2023
Gestione Strumentazione	

Sistema Halia	2023
Reti per l'integrazione sul territorio	
Integrazione DNLAB/Progetto Regionale Escape + sistema di monitoraggio	2023
Sistemi di Reparto e di Gestione dei ricoveri	
Sistema Hero (Repository, Portale referti, ADT, Order Entry)	2023
Sistema Oncosys	2023
Modulo cartella clinica medica di reparto (4 reparti)	2023
Modulo cartella clinica medica di reparto (12 reparti)	2023
BI - BI4H-DATA PLATFORM (Direzione Scientifica)	2023
P4C Therapy	2023
NUOVA IMPLEMENTAZIONE	
Cartella Clinica e Terapia Intensiva (TI)	
Sviluppo TI Fase 1 - Gestione Attività Mediche + Collegamento degli apparecchi	2023
Sviluppo TI Fase 2 - Dashboard ICU + Scheda infermieristica	2024
Sale Operatorie	
Servizi Porting dalla piattaforma Ormaweb alla piattaforma O4C (blocco operatorio)	2023
Rilevazione dei tempi operatori di spostamento in tempo reale Consolidamento cruscotto di monitoraggio delle sedute operatorie	2024
Integrazione con le apparecchiature di anestesia (Monitor e ventilatori) - In carico agli IFO: Sistema Concentratore che gestisce il collegamento dei monitor e dei ventilatori	2024
Attivazione BI evoluta per l'attività sulle sale operatorie	2024
Copia Cartella Clinica	
Richiesta, pagamento e ritiro copia della Cartella Clinica tramite app	2023
Interoperabilità	
Piattaforma di Interoperabilità – Repository Fhir e Patient Synoptic	2023
Smart Imaging	

- **Evoluzione Anatomia Patologica [codice 06-02]**

Gli IFO dispongono di un sistema gestionale di Anatomia patologica che permette di gestire il workflow dell'analisi di laboratorio del campione dal momento della richiesta dal blocco chirurgico a quello della predisposizione del referto, tracciando puntualmente le varie fasi prodromiche al referto, comprese quelle di utilizzo delle varie strumentazioni, della gestione del vetrino, ecc.

Il referto una volta firmato digitalmente è reso consultabile dai medici richiedenti accedendo all'applicativo di cartella clinica.

Ovviamente, non è consentito in alcun modo accedere al referto in consultazione sino alla sua validazione.

Il tracciamento applicativo comprende anche le fasi, come detto, di gestione del vetrino, dalla scansione al processo univoco di identificazione attraverso imprinting laser.

Il sistema dovrà evolvere in modo tale da consentire la predisposizione della richiesta di analisi anche dagli ambulatori attraverso specifico modulo di Order Entry.

- **Gestione dei sistemi interni di prenotazione [codice 06-03]**

Si prevede di evolvere le Piattaforme attuali che consentono le prenotazioni delle prestazioni di Medicina nucleare e di Radiologia.

Alle Piattaforme è collegato un modulo per la ricetta dematerializzata che si interfaccia con la Piattaforma regionale e un modulo per l'invio degli sms agli assistiti.

- **Piattaforma di Radioterapia [codice 06-04]**

Presso la Radioterapia Oncologica degli IFO è in uso una Piattaforma che permette la gestione clinica elettronica ambulatoriale multidisciplinare collegata ai moduli

Sono previste attività evolutive di integrazione, sviluppo ed evoluzione per consentire:

- la discussione clinica del paziente, classificazione della priorità, messa in lista con calcolo dell'avanzamento automatico in base ai parametri clinici e calcolo previsionale della data effettiva di inizio terapia in base ai dati di trattamento importati tramite HL7 dal sistema gestionale oncologica;
- l'esecuzione di procedure di controllo di qualità delle prestazioni erogate e rendicontate manualmente prima del processo di prescrizione con meccanismi di automatismo di warning e mailing interno ai responsabili del controllo qualità
- Evoluzione e sviluppo di algoritmi complessi di controllo qualità della rendicontazione, in base a dati di dose, numero di immagini, e archi provenienti dall'importazione automatica HL7 dei dati di trattamento di ARIA.
- Evoluzione della prescrizione dematerializzata per la trasmissione delle impegnative, al fine di consentire l'erogazione (che innesca il rimborso regionale) tramite file, su tracciato personalizzato e documenti di accompagnamento di riepilogo che facilitino il riscontro manuale e automatico.
- Realizzazione e supporto alle procedure di creazione/aggiornamento anagrafica pazienti della Piattaforma Oncologica mediante interfaccia HL7 collegata ai sistemi gestionali operanti in IFO previa fattibilità tecnica.
- Personalizzazione della meta cartella clinica ambulatoriale EMR, con aggiunta delle schede di compilazione assistita delle informazioni cliniche essenziali per la prima visita, simulazione, visite durante trattamento e visite di follow-up.
- Reportistica per l'analisi dei dati dei pazienti estratti per patologia, stadiazione, tipo trattamento, tolleranze al trattamento ed esiti
- Reportistica per l'analisi dei volumi delle prestazioni erogate.

PARTE IIIa - La governance

CAPITOLO 7. Governance

a) Governance sistemi IT: Framework della Sicurezza informatica e della protezione dei dati in IFO

Il framework prevede, in particolare, di implementare un SGSI in un orizzonte temporale di 36 mesi, adottando misure che possono essere sintetizzati in 4 prospettive fondamentali:

1. analisi e indirizzo, per supportare la definizione dei processi, lo sviluppo di metodologie e di metriche valutative per il governo del sistema;
2. iniziative di formazione e comunicazione, per promuovere la cultura della sicurezza cibernetica, favorendo il grado di consapevolezza (awarness) e competenza all'interno degli Istituti attraverso la condivisione di informazioni relative a specifici eventi in corso, nuovi scenari di rischio o specifiche tematiche di sicurezza delle informazioni.
3. interventi proattivi, aventi come scopo la raccolta e l'elaborazione di dati significativi ai fini della sicurezza quali ad es. analisi delle minacce e delle vulnerabilità, monitoraggio dei bollettini e delle segnalazioni di sicurezza, implementazione e gestione di basi di dati informative;
4. interventi reattivi, aventi come scopo la gestione degli allarmi di sicurezza, il supporto ai processi di gestione e la risoluzione degli incidenti di sicurezza all'interno del dominio degli istituti;

Le azioni si declinano in interventi da attuare necessariamente a diversi livelli distinguendo tra sicurezza organizzativa, logica e fisica per incrementare la capacità di resilienza del sistema nel suo complesso. Risulta peraltro opportuno che le soluzioni di sicurezza adottate (tecnologica, organizzativa e logistica) in tema di strutture informative risultino quanto più armoniche ed omogenee possibile con quelle assunte o da assumere in materia di protezione dei dati personali al fine di rendere il sistema flessibile ed idoneo per gli scopi assegnati.

Da un punto di vista organizzativo sono da prevedere misure di prevenzione atte a ridurre il rischio di attacchi cibernetici anche con l'adozione di policy finalizzate a far assumere maggiore consapevolezza dei rischi derivanti da comportamenti non adeguati e comunque non in linea alle policy aziendali.

La sensibilizzazione sarà attuata attraverso momenti di formazione in aula, erogazione di specifici corsi e-learning e consultazione sistematica delle piattaforme rese disponibili a livello nazionale e non (si fa riferimento ad esempio al National Vulnerability Database gestito

tramite la piattaforma Infosec già a disposizione di tutte le amministrazioni in sola consultazione).

E' previsto inoltre di aumentare la capacità di difesa, con l'adozione di scelte architetturali volte a ridurre la "superficie di attacco" e con l'acquisizione di dispositivi hardware e software mirati ad innalzare il livello di protezione in accordo alle Direttive ACN.

Il Framework si fonda sulle seguenti Attività (che corrispondono alle Category del Cybersecurity Framework NIST):

- Asset Management
- Risk Analysis
- Configuration Management
- Operational Planning
- Piano di Formazione e di informazione
- Interventi di prevention
- Interventi operativi per la gestione dell'incidente

Di seguito si riporta una descrizione schematica di ciascuna attività.

1. Asset Management

Attività	1. Asset Management
Risponde alla domanda	*Cosa devo proteggere*
Oggetto	*Identificare le risorse aziendali potenziali target di attacchi cibernetici e di altro tipo: dispositivi perimetrali, hw, sw, documenti cartacei/informatici, dati applicativi*
Responsabile	*RTD*
Accountable	*CISO*
Support	*RPCT*
Consulted	*DPO*
Informed	*Direttore Amministrativo, Direttori Sanitari, Responsabile della Conservazione sostitutiva, Responsabile dei flussi documentali, Responsabili degli archivi*
Riferimenti	*NIST Cybersecurity Framework, COBIT, Standard ISO/IEC 27002, Standard ISO/IEC 27001:2013, , ISO/IEC 27031:2011*
Vincoli	*Condivisione degli obiettivi con il Management aziendale*
Output	*Asset Inventory, Registro dei trattamenti*

2. Risk Analysis

Attività	2. Risk Analysis
Risponde alla domanda	*Quali sono gli elementi di rischio*
Oggetto	*Individuare i rischi e le vulnerabilità per ogni risorsa precedentemente individuata. L'attenzione è rivolta alla codifica di due processi. Il primo è il Risk Assessment che è la valutazione (probabilistica) dei rischi aziendali, a questa fase segue il Risk Management che è il processo mediante il quale si sviluppano le strategie necessarie a mitigare, eliminare e monitorare i rischi.*
Responsabile	*RTD*
Accountable	*CISO*
Support	*Owner dei processi*
Consulted	*DPO*
Informed	*RPCT, Direttore Amministrativo, Direttori Sanitari, Responsabile della Conservazione sostitutiva, Responsabile dei flussi documentali, Responsabili degli archivi*
Riferimenti	*IEC 31010:2019, ISO 31000:2018, ISO Guide 73:2009, ISO/IEC 27031:2011*
Vincoli	*Esecuzione dell'attività 1, Conoscenza dei processi e delle procedure aziendali*
Output	*Risk register, Registro dei trattamenti, BPIA*

3. Configuration Management

Attività	3. Configuration Management
Risponde alla domanda	*Come utilizzare al meglio le risorse*
Oggetto	*Per ogni risorsa individuare l'ambiente di utilizzo e le modalità di transizione ad altra configurazione*
Responsabile	*RTD*

Accountable	*CISO*
Support	*Owner dei processi*
Consulted	*DPO*
Informed	*RPCT, Direttore Amministrativo, Direttori Sanitari, Responsabile della Conservazione sostitutiva, Responsabile dei flussi documentali, Responsabili degli archivi*
Riferimenti	*ISO 10007:2017, ITIL, COBIT*
Vincoli	*Esecuzione dell'attività 1*
Output	*Configuration Control Process*

4. Operational Planning

Attività	**4. Operational Planning**
Risponde alla domanda	*Cosa faccio prima in relazione alle criticità e alle priorità della vision aziendale*
Oggetto	*Stabilire il piano di azione in relazione agli elementi raccolti nella fase precedente*
Responsabile	*RTD*
Accountable	*CISO*
Support	*Direttore Amministrativo*
Consulted	*DPO*
Informed	*RPCT, Direttore Amministrativo, Direttori Sanitari, Responsabile della Conservazione sostitutiva, Responsabile dei flussi documentali, Responsabili degli archivi*
Riferimenti	*ISO/IEC 9001:2015*
Vincoli	*Esecuzione dell'attività 1*
Output	*Baseline di Progetto*

5. Piano di Formazione e di informazione

Attività	**5. Piano di Formazione e di informazione**
Risponde alla domanda	*Come faccio a disporre di persone adatte al raggiungimento degli obiettivi*
Oggetto	*Predisporre un Piano di formazione e di informazione da destinare a personale, addetti e collaboratori. L'analisi degli attacchi informatici rilevano come la maggior parte sia dovuta a comportamenti non adeguati da parte del personale e dalla mancanza di procedure codificate di Policy. La formazione e la sensibilizzazione dei dipendenti sui rischi informatici ricoprono un ruolo chiave per la prevenzione degli attacchi e possono essere attuati anche in parallelo alla definizione del Modello di sicurezza.*
Responsabile	*Direttore Amministrativo*
Accountable	*Responsabile della formazione*
Support	*Responsabile Risorse umane*
Consulted	*DPO*
Informed	*RPCT, Direttore Amministrativo, Direttori Sanitari, Responsabile della Conservazione sostitutiva, Responsabile dei flussi documentali, Responsabili degli archivi*
Riferimenti	*UNI ISO 21001:2019*
Vincoli	*Esecuzione dell'attività 1*
Output	*Piano di Formazione e comunicazione*

Interventi di prevention

Attività	6. Interventi di prevention		
	Sicurezza organizzativa	**Sicurezza perimetrale**	**Sicurezza dei server**
Risponde alla domanda	*Come riduco i rischi derivanti dalla presenza quotidiana di personale, collaboratori, addetti esterni, pazienti, visitatori*	*Come riduco i rischi di inoculazione di elementi informatici potenzialmente dannosi*	*Come riduco i rischi di vulnerabilità dei sistemi server presenti nella mia organizzazione*
Oggetto	*Definire una Policy che miri, pur nel rispetto del servizio pubblico assicurato dall'Azienda, a isolare e proteggere le risorse più critiche attraverso la loro disposizione in aree di minor accesso al pubblico e ricorrendo a dispositivi anti-intrusione (anche controlli di accesso laddove necessario) per consentire il passaggio alle sole persone abilitate. Si tratta pertanto di individuare misure organizzative che diano indicazioni alla logistica per una più adeguata allocazione delle risorse (dispositivi di rete, end point, archivi di referti e di cartelle cliniche...). Saranno da studiare misure che consentano anche il monitoraggio dei parcheggi e la possibilità di consentire il parcheggio interno ai pazienti e ai loro parenti adeguatamente registrati. Rientrano in tale categoria, anche le modalità di codifica delle procedure e dei processi concernenti la sicurezza, l'individuazione di compiti e responsabilità, le misure per la protezione dei dati da eventi di origine naturale o dolosa (antincendio, allagamento, ...) o le misure per la protezione da condizioni ambientali proibitive o da eventuali riduzioni dell'efficienza dei sistemi di supporto (impianti ausiliari).*	*Impostare una politica tesa alla protezione del sistema informativo degli IFO da accessi non autorizzati dall'esterno, con particola riferimento al contrasto degli attacchi informatici condotti attraverso la rete Verifica delle componenti IDS e IPS per identificare e bloccare i port scan, e a componenti di proxy server e content filtering.*	*Definire Policy per la corretta gestione dei dispositivi server con particolar riferimento alle modalità di designazione degli utenti administrator, delle configurazioni più adatte per impedire l'accesso a file e applicazioni, valutare l'opportunità di disabilitare alcuni protocolli (ad es. protocollo SMB per evitare crittografie di dati da parte di utenti smaliziati), disciplinare le modalità di aggiornamento dei firmware, collocare i server in ambienti adeguati per proteggerli da accessi fisici non autorizzati e da eventuali problemi di natura ambientale/climatica.*
Responsabile	*Direttore Amministrativo*	*RTD*	*RTD*
Accountable	*Responsabile della sicurezza aziendale*	*CISO*	*CISO*
Support	*Logista*	*Fornitori, CERT-PA, Regione*	*Fornitori, CERT-PA, Regione, ACN*
Consulted	*DPO*	*DPO*	*DPO*
Informed	*RPCT, Direttore Amministrativo, Direttori Sanitari, Responsabile della Conservazione sostitutiva, Responsabile dei flussi documentali, Responsabili degli archivi*	*RPCT, Direttore Amministrativo, Direttori Sanitari, Responsabile della Conservazione sostitutiva, Responsabile dei flussi documentali, Responsabili degli archivi*	*RPCT, Direttore Amministrativo, Direttori Sanitari, Responsabile della Conservazione sostitutiva, Responsabile dei flussi documentali, Responsabili degli archivi*
Riferimenti	*ISO 27001:2017, ISO/IEC 27032:2012*	*ISO 27001:2017, ISO/IEC 27033:2016, ISO/IEC 27036:2016*	*ISO 27001:2017, ISO/IEC 27040:2017, ISO/IEC 27033:2016, ISO/IEC 27036:2016*
Vincoli	*Esecuzione dell'attività 1*	*Esecuzione dell'attività 1*	*Esecuzione dell'attività 1*
Output	*Piano di sicurezza, Risk Register, Registro dei trattamenti, BPIA*	*Vulnerability assessment, Linee guida per la predisposizione dei capitolati e l'esecuzione dei collaudi*	*Vulnerability assessment, Linee guida per la predisposizione dei capitolati e l'esecuzione dei collaudi*
Attività	**6. Interventi di prevention**		

	Sicurezza CLOUD	Sicurezza dispositivi utente	Sicurezza dispositivi sanitari
Risponde alla domanda	*Come riduco i rischi di vulnerabilità dei sistemi CLOUD*	*Come riduco i rischi di vulnerabilità dei dispositivi utente*	*Come riduco i rischi di utilizzo di applicazioni non sicure*
Oggetto	*Attuare una Policy che, sulla base delle Linee guida diramate dal CERT Nazionale, definisca le modalità operative da adittare per la scelta e l'attivazione dei servizi CLOUD. I rischi derivano dalla gestione esternalizzata di servizi/risorse e dal luogo fisico di gestione del CLOUD, per definire il quadro legislativo di riferimento. Importante la defnizione delle regole contrattuali da prevedere e le interrelazioni con l'ambito Privacy, per gli aspetti correlati alla nomina del Responsabile esterno del Trattamento. Richiedere sempre le misure adottate dal fornitore per quanto concerne l'adozione di soluzioni compliant alla sicurezza e alla privacy by design/by default, i penetration test o i stress test che devono essere assicurati con periodicità, essere informati sugli stack applicativi e sulle componenti software utilizzate (anche come versioni) in modo da poter chiedere conto degli aggiornamenti effettivamente eseguiti. La fornitura delle informazioni deve pervenire in modo periodico e secondo procedure concordate che prevedono la firma elettronica come "certificazione" dei dati.*	*Impostare una politica che sia orientata a ricorrere per i sistemi utilizzati dagli utenti (pc, stampanti di rete, smartphone, tablet,…)all'installazione di Sistemi Antivirus, anche abbinati a Personal firewall, e a Sistemi Data Loss Prevention - comprendendo in essi anche il ricorso alla crittografia - e programmazione di aggiornamento e di installazione di patch.*	*Attuare una Policy per assicurare la maggior sicurezza possibile sull'uso e sulle attività di manutenzione dei dispositivi, anche in relazione alle crescenti attività che vengono svolte in modalità remota. Prevedere una procedura codificata per la verifica della configurazione e per assicurare il puntuale monitoraggio del dispositivo dal suo ingresso in azienda sino alla sua dismissione. La Policy deve essere conforme agli standard in vigore e anche alle linea guida "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices" (Food and Drug Administration USA) contenente aggiornamenti relativi ai requisiti di gestione della sicurezza informatica dei dispositivi medici dotati di software. In particolare, la compliance si richiede per il sistema di categorizzazione dei rischi relativi alla sicurezza informatica basato su due livelli. Richiedere sempre le misure adottate dal fornitore per quanto concerne l'adozione di soluzioni compliant alla sicurezza e alla privacy by design/by default, i penetration test o i stress test che devono essere assicurati con periodicità, essere informati sugli stack applicativi e sulle componenti software utilizzate (anche come versioni) in modo da poter chiedere conto degli aggiornamenti effettivamente eseguiti. La fornitura delle informazioni deve pervenire in modo periodico e secondo procedure concordate che prevedono la firma elettronica come "certificazione" dei dati.*
Responsabile	*RTD*	*RTD*	*RTD*
Accountable	*CISO*	*CISO*	*CISO*
Support	*Fornitori, CERT-PA, Regione*	*Fornitori, CERT-PA, Regione*	*Fornitori, Regione*
Consulted	*DPO*	*DPO*	*DPO*
Informed	*RPCT, Direttore Amministrativo, Direttori Sanitari, Responsabile della Conservazione sostitutiva, Responsabile dei flussi documentali, Responsabili degli archivi*	*RPCT, Direttore Amministrativo, Direttori Sanitari, Responsabile della Conservazione sostitutiva, Responsabile dei flussi documentali, Responsabili degli archivi*	*RPCT, Direttore Amministrativo, Direttori Sanitari, Responsabile della Conservazione sostitutiva, Responsabile dei flussi documentali, Responsabili degli archivi*
Riferimenti	*ISO 27001:2017, ISO/IEC 27040:2017, , ISO/IEC 27033:2016, ISO/IEC 27036:2016, CLASP, STRIDE*	*ISO 27001:2017, ISO/IEC 27036:2016, Security Development Lifecycle, CLASP, STRIDE*	*ISO 27001:2017, ISO/IEC 27040:2017, ISO/IEC 27031:2011, , ISO/IEC 27036:2016, Security Development Lifecycle, CLASP, STRIDE*
Vincoli	*Esecuzione dell'attività 1*	*Esecuzione dell'attività 1*	*Esecuzione dell'attività 1*
Output	*Vulnerability assessment, Linee guida per la predisposizione dei capitolati e l'esecuzione dei collaudi*	*Vulnerability assessment, Linee guida per la predisposizione dei capitolati e l'esecuzione dei collaudi*	*Vulnerability assessment, Linee guida per la predisposizione dei capitolati e l'esecuzione dei collaudi*

Attività	6. Interventi di prevention	
	Sicurezza applicativa	**Sicurezza dati**
Risponde alla domanda	*Come riduco i rischi di utilizzo di applicazioni non sicure*	*Come riduco i rischi di una esfiltrazione di dati da parte degli utenti interni*
Oggetto	*Impostare una politica di sviluppo software o di acquisizione software basata su attività di monitoraggio delle procedure di sviluppo/realizzazione imperniate sulla security by design (graditi ricorsi a modelli CLASP), della documentazione e delle modalità di autenticazione anche incentivando il ricorso a SPID. Richiedere sempre le misure adottate dal fornitore per quanto concerne l'adozione di soluzioni compliant alla sicurezza e alla privacy by design/by default, i penetration test o i stress test che devono essere assicurati con periodicità, essere informati sugli stack applicativi e sulle componenti software utilizzate (anche come versioni) in modo da poter chiedere conto degli aggiornamenti effettivamente eseguiti. La fornitura delle informazioni deve pervenire in modo periodico e secondo procedure concordate che prevedono la firma elettronica come "certificazione" dei dati trasmessi.*	*Attivare una Policy che prevede che, per le tipologie di dati classificati o comunque ritenuti sensibili, si attui una duplicazione degli stessi. La Policy è correlata alla gestione del data breach, in generale, ed è quindi da raccordare con le misure adottate per la privacy.Gli interventi si concretizzano in una gestione del dato ridondante "mirata" e ad attuare procedure di tracciamento puntuale di accessi ai dati medesimi. Evidenti le interrelazioni con gli interventi per l'autenticazione e la profilazione degli utenti.*
Responsabile	*RTD*	*RTD*
Accountable	*CISO*	*CISO*
Support	*Fornitori, CERT-PA, Regione*	*Fornitori, CERT-PA, Regione*
Consulted	*DPO*	*DPO*
Informed	*RPCT, Direttore Amministrativo, Direttori Sanitari, Responsabile della Conservazione sostitutiva, Responsabile dei flussi documentali, Responsabili degli archivi*	*RPCT, Direttore Amministrativo, Direttori Sanitari, Responsabile della Conservazione sostitutiva, Responsabile dei flussi documentali, Responsabili degli archivi, Diretti interessati*
Riferimenti	*ISO 27001:2017, ISO/IEC 27034:2018, ISO/IEC 27031:2011, ISO/IEC 27036:2016, Security Development Lifecycle, CLASP, STRIDE*	*ISO 27001:2017, ISO/IEC 27040:2017, ISO/IEC 27033:2016, , ISO/IEC 27031:2011*
Vincoli	*Esecuzione dell'attività 1*	*Esecuzione dell'attività 1*
Output	*Vulnerability assessment, Linee guida per la predisposizione dei capitolati e l'esecuzione dei collaudi*	*Vulnerability assessment, Linee guida per la predisposizione dei capitolati e l'esecuzione dei collaudi*

7. Interventi operativi per la gestione dell'incidente

Attività	7. Interventi operativi per la gestione dell'incidente		
	Detect and identification	**Incident Management**	**Follow up**
Risponde alla domanda	*Come mi attivo di fronte ad un attacco cibernetico*	*Come gestisco un attacco cibernetico*	*Come opero dopo che l'emergenza è cessata*
Oggetto	*Organizzare una Task force (SOC+Cert) per la detection ed analisi predittiva nonché per la preventiva gestione di alert che segnalano la possibilità di un attacco cibernetico. I componenti sono individuati formalmente i componenti della Task force e ad ognuno di essi è affidato un compito con le relative responsabilità. Sono peraltro dotati di dispositivi per essere immediatamente contattati 24h e per poter agire anche in remoto. E' individuata una sala regia dove convergere in caso di necessità ed una sede di backup nel caso la prima sede non sia raggiungibile.*	*Per gestione degli incidenti, si fa riferimento a qualsiasi azione mirata ad attaccare una risorsa informativa o IT dell'Azienda. A tal fine è necessario attuare una Procedura codificata che definisca le attività che la Task force debba avviare per ripristinare le condizioni di normalità nel tempo più breve possibile e ridurre l'impatto sui servizi erogati dall'Azienda, sugli stakeholder e sulla reputation dell'organizzazione. La procedura da adottare può essere una personalizzazione del Modello ITIL. Si auspica un accordo con AgID per disporre del supporto della struttura del Cert-PA da disciplinare in un contesto di collaborazione più ampio.*	*Definire una Policy di Lesson learned e di alimentazione delle basi dati informative di riferimento. La componente CERT relaziona il management attraverso i dati derivanti dalla detection effettuata dal SOC, rispetto a quanto accaduto evidenzia le vulnerabilità che hanno consentito all'attaccante di sfruttare le debolezze del sistema e definisce un Piano di miglioramento per mitigare i rischi derivanti dalla o dalle vulnerabilità interessate.*
Responsabile	*RTD*	*RTD*	*RTD*
Accountable	*CISO*	*CISO*	*CISO*
Support	*Fornitori, CERT-PA, Regione*	*Fornitori, CERT-PA, Regione, Garante Privacy, Polizia postale*	*Fornitori, CERT-PA, Regione*
Consulted	*DPO*	*DPO*	*DPO*
Informed	*RPCT, Direttore Amministrativo, Direttori Sanitari, Responsabile della Conservazione sostitutiva, Responsabile dei flussi documentali, Responsabili degli archivi, Diretti interessati*	*RPCT, Direttore Amministrativo, Direttori Sanitari, Responsabile della Conservazione sostitutiva, Responsabile dei flussi documentali, Responsabili degli archivi, Diretti interessati*	*RPCT, Direttore Amministrativo, Direttori Sanitari, Responsabile della Conservazione sostitutiva, Responsabile dei flussi documentali, Responsabili degli archivi*
Riferimenti	*ISO 27001:2017, ISO/IEC 27043:2017, ISO/IEC 27035:2016*	*ISO/IEC 27031:2011, ISO 27001:2017, ISO/IEC 27043:2017, ISO/IEC 27035:2016*	*ISO 27001:2017, ISO/IEC 27043:2017, ISO/IEC 27035:2016, , ISO/IEC 27031:2011, , ISO/IEC 27036:2016*
Vincoli	*Esecuzione dell'attività 1*	*Esecuzione dell'attività 1 e dell'attività 13*	*Esecuzione dell'attività 1 e dell'attività 14*
Output	*Incident Register, Convocazione Task force, Piano di emergenza*	*Incident Register, Operatività Task force, Piano di emergenza, chiusura dell'incidente, segnalazioni ad Autorità competenti*	*Piano delle Lesson Learned, Piano di Miglioramento, Piano Operativo, Piano di formazione e comunicazione*

b) Governance Sanità Digitale: coordinamento delle attività per l'implementazione dei Progetti finanziati in ambito PNRR e PNC

Il piano di programmazione regionale (Programmi Operativi di cui alla DGR 406 del 26 giugno 2020 riguardante il "Piano di riorganizzazione, riqualificazione e sviluppo del Servizio Sanitario Regionale 2019-2021, come integrato con i Programmi Operativi 2022-2024) intende proseguire, implementare e completare la strategia e le azioni necessarie per il raggiungimento di obiettivi specifici che concorrono alla programmazione degli investimenti nella Sanità del Lazio con l'utilizzo dei fondi del Piano Nazionale di Ripresa e Resilienza (PNRR) e del Piano Nazionale Complementare (PNC).

Con la deliberazione della Giunta regionale del 9 novembre 2021, n. 755, è stata pertanto emanata la "Governance operativa regionale per l'attuazione del Piano Nazionale di Ripresa e Resilienza (PNRR) e del Piano Nazionale Complementare al PNRR (PNC)" a cui è poi seguita l'istituzione di una Cabina di Regia, che, in stretta correlazione ed in continuità ai compiti degli altri gruppi di lavoro regionali, opera per il rilevamento dello stato di attuazione degli interventi delle diverse linee di investimento previste dalla Missione 6 Salute e della Missione 1 del PNRR, anche nell'ottica di favorire l'implementazione di una strategia unitaria regionale in materia di innovazione tecnologica e trasformazione digitale e nonché di assicurare la coerenza tra gli interventi e il coordinamento dei progetti che dovranno essere realizzati dai Soggetti attuatori delegati.

La Regione difatti gestisce molte delle piattaforme informatiche strategiche utilizzate dalle ASL/AO ed assume pertanto un ruolo fondamentale nelle attività correlate al raggiungimento degli obiettivi di Sanità Digitale, fornendo anche le indicazioni strategiche cui attenersi.

I gruppi di lavoro e la citata Cabina di regia costituiscono le principali modalità di interazione: gli strumenti/interventi per il coinvolgimento del territorio sulle iniziative autonome sono costituiti in massima parte dalle Piattaforme Social, considerato che gli IFO rappresentano eccellenze nazionali a livello oncologico (Istituto Regina Elena – IRE) e dermatologico (Istituto San Gallicano – ISG).

Le modalità di *governance* adottate dal RTD si basano su gruppi di lavoro multidisciplinari costituiti da personale sanitario ed amministrativo, che operano con tecniche di Project Management per assicurare il continuo monitoraggio dello sviluppo delle linee d'azione, la rilevazione a cadenza stabilita i SAC e dei SAL per l'eventuale intercetto dei ritardi al fine di individuare tempestivamente e rimuovere le cause che hanno determinato gli sfasamenti temporali.

Contesto normativo e strategico

Specificare riferimenti normativi e strategici a cui l'amministrazione devono attenersi.

Riferimenti normativi italiani: non applicabile

Riferimenti normativi europei: non applicabile

Obiettivi e risultati attesi

- implementare il Piano operativo
- assicurare il continuo monitoraggio dello sviluppo delle linee d'azione

Cosa deve fare l'Amministrazione

- definire il team di monitoraggio individuando ruoli e responsabilità
- rilevazione a cadenza stabilita i SAC e dei SAL
- gestione Open Point

APPENDICE 1. Acronimi

Acronimo	Definizione
AGID	Agenzia per l'Italia Digitale
ANPR	Anagrafe nazionale popolazione residente
API	Application Programming Interface
CAD	Codice dell'amministrazione digitale

Si consideri la tabella riportata a titolo esemplificativo e non esaustivo.