Allegato X

Integrazione di Sistemi Software Clinici con il Sistema Informativo Sanitario Provinciale

Marco Foracchia, 20151208
r1 - Mauro Barani, 20160302
r2 – Federica Garlassi 20210513

Il presente documento descrive i requisiti e le modalità di Integrazione dei sistemi informativi clinici (intesi come sistemi comprensivi di dispositivi hardware e software la cui destinazione d'uso sia legate al supporto dei processi clinici attraverso il trattamento di dati sanitari) nel sistema informativo sanitario della provincia di Reggio Emilia (**SISP**) per quanto di pertinenza dell'Azienda USL di Reggio Emilia (**AUSL**).

Il documento è orientato a interlocutori tecnici del settore IT / ingegneria clinica e costituisce quadro di capitolato (vincolo contrattuale) o regolamento (vincoli aziendali) relativamente alla adozione e attivazione dei sistemi informativi clinici.

Il coordinamento delle attività di integrazione col SISP sarà svolto congiuntamente dal Servizio di Ingegneria Clinica (**INGCLIN**) e Servizio Tecnologie Informatiche e Telematiche (**STIT**).

Quanto descritto nel presente documento potrebbe non applicarsi interamente a tutti i contesti. Allegato a questo documento, potrebbe essere consegnata una **Scheda di Integrazione** (Allegato X.0) che indica in modo sintetico e riassuntivo quali integrazioni (hardware, rete, sistemistici e integrazione applicativa), tra quelle descritte nel presente documento, sono previste per lo specifico sistema informativo. Qualora non fosse disponibile, si assume che il sistema informativo in oggetto debba integrarsi rispettando, quando applicabili, tutte le disposizioni previste nel presente documento.

Indipendentemente dal livello di integrazione del sistema informativo nel SISP, è richiesta la compilazione **Scheda Sintetica di Descrizione del Sistema Informativo** (Allegato X.9), che riassume la rispondenza del sistema ai requisiti definiti nel presente documento.

Il presente documento non tratta eventuali vincoli derivanti dalla classificazione del sistema software come Dispositivo Medico (Rif. disciplina relativa vigente). Tali vincoli sono oggetto di verifica da parte di INGLIN, indipendente dal livello di integrazione del software all'interno del sistema informativo sanitario provinciale.

Il presente documento non tratta eventuali vincoli derivanti dalla trasmissione dati verso l'esterno dell'azienda (es. soluzioni "cloud"). Questo ambito, essendo la normativa specifica ancora in evoluzione, deve essere trattato in modo specifico con lo STIT attraverso valutazioni della soluzione proposta.

Nel presente documento sono trattati:

- Requisiti Minimi di Sicurezza del sistema (identificati con sigla RP)
- Requisiti di Rete e Sistemistici (identificati con sigla RS)
- Requisiti di Integrazione coi principali componenti del Sistema Informativo Sanitario provinciale (identificati con sigla RI)
- Requisiti Aggiuntivi (identificati con sigla RA)
- Modalità di Collaudo

1 Requisiti Minimi di Sicurezza

Di seguito sono descritti i requisiti minimi di sicurezza che ciascun sistema software deve soddisfare per la sua adozione presso le aziende sanitarie pubbliche della provincia di Reggio Emilia. I requisiti descritti costituiscono vincoli indotti dalla attuale normativa sul Trattamento Dati Sensibili (Rif. disciplina Privacy vigente).

Il fornitore deve inoltre fornire autocertificazione di conformità al Regolamento Europeo (GDPR) e alla Legge 196/2003 e s.m.i, e aderenza alle Misure Minime di Sicurezza ICT per le pubbliche Amministrazioni (al livello minimo) emesse con Direttiva del Presidente del Consiglio dei Ministri in data 1 agosto 2015.

Qualora il sistema offerto o già acquistato dall'azienda non fosse conforme ad uno o più dei requisiti descritti, è necessario che sia specificato nella apposita sezione della Scheda Sintetica di Descrizione del Sistema Informativo, specificando il motivo della non-conformità (es. sistema classificato come DM di produzione estera, non immediatamente adeguabile alla normativa vigente in Italia). Le non conformità sono oggetto di verifica in fase di collaudo, e deroga previa dichiarazione firmata di presa di responsabilità del fornitore qualora la motivazione fosse ritenuta accettabile.

1.1 Confidenzialità del Dato

- **RP1**. Il sistema informativo deve prevedere autenticazione tramite username e password personali con valore minimo di 8 caratteri o 14 caratteri per le utenze amministrative (o altra metodologia più forte in relazione alla classificazione fatta dal Codice Amministrazione Digitale (CAD) e alle Misure Minime di Sicurezza ICT).
- **RP2.** Il sistema deve prevedere la scadenza periodica della password personale e impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo, con periodicità in linea con la disciplina Privacy e di Misure Minime di Sicurezza ICT vigenti.
- **RP3**. Il sistema di autenticazione deve prevedere integrazione con i server di autenticazione aziendale, basati su ActiveDirectory (tramite protocollo LDAPS o autenticazione integrata).
- **RP4**. Il sistema deve prevedere la profilazione degli utenti abilitati al sistema, consentendo agli utenti classificati come "amministratori di sistema" di limitare le possibilità di accesso degli utenti a singole sezioni/funzionalità del sistema stesso.
- **RP5.** Il sistema deve utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi e non per la normale operatività, come da Misure Minime di Sicurezza ICT vigenti.
- **RP6.** Il ruolo di "amministratori di sistema" deve essere assegnabile anche a utenti di AUSL (non vincolato ai soli utenti di supporto fornitore).
- **RP7.** Il sistema deve prevedere la tracciabilità di tutti gli accessi al sistema, indicando in particolare il contesto clinico a cui si è fatto acceso (es. riferimento al paziente i cui dati sono stati oggetto di

consultazione/modifica, identificazione del dato consultato/modificato) e identificare quando si opera con privilegi amministrativi.

- **RP8.** Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per contesti di emergenza e devono essere riconducili a chi le ha utilizzate, come da Misure Minime di Sicurezza ICT vigenti.
- **RP9.** Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona, come da Misure Minime di Sicurezza ICT vigenti
- **RP10.** Il sistema deve garantire che le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature siano eseguite per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri), come da Misure Minime di Sicurezza ICT vigenti.

1.2 Integrità del Dato

- **RP11.** Il sistema deve prevedere archiviazione esclusivamente su server (nessun dato archiviato su client/workstation).
- **RP12.** Il sistema deve impedire o limitare fortemente l'utilizzo di dispositivi esterni a quelli necessari per il funzionamento, oltre a disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi rimuovibili, come da Misure Minime di Sicurezza ICT vigenti.
- **RP13.** Il sistema deve prevedere sistema di backup dati (o appoggiarsi su sistemi di backup aziendali, vedi di seguito), che preveda almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema al di fuori del sistema originario, come da Misure Minime di Sicurezza ICT vigenti.
- RP14. – Il sistema deve assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura, come da come da Misure Minime di Sicurezza ICT vigenti.
- **RP15.** Il fornitore deve prevedere, come parte integrante della fornitura, servizi di Test di Restore da backup, con cadenza minima annuale.**RP16.** Il sistema deve prevedere sistema antivirus e antimalware, con relativi sistemi di aggiornamento automatico delle firme (o appoggiarsi sui sistemi antivirus aziendali, vedi di seguito) e ove possibile scansione real-time, come da Misure Minime di Sicurezza ICT vigenti.
- **RP17.** Il sistema deve prevedere aggiornamenti automatici relativi alla sicurezza (o gestiti manualmente dal fornitore, in tal caso devono essere compresi in fornitura i servizi) dei principali componenti di sistema operativo e di firmware ai più recenti aggiornamenti di sicurezza (es. patch di sistema operativo).
- **RP18.** Il fornitore deve prevedere che a seguito di segnalazione di vulnerabilità emerse dalle scansioni o da comunicazioni ufficiali, siano previste ed attuabili tutte le contromisure atte a garantire protezione del sistema, ad es. per mezzo di patch specifiche, oppure documentando e dichiarando il livello di rischio ritenuto accettabile nel contesto operativo, come da Misure Minime di Sicurezza ICT vigenti.

1.3 Continuità e Disponibilità del Dato

- **RP19.** Per ogni funzionalità del sistema che sia ritenuta critica (come da definizione fornita con gli SLA richiesti per il sistema), devono essere forniti adeguati dispositivi hardware e strumenti software di backup funzionale che consentano, in caso guasto, di garantire la continuità operativa del sistema o comunque il ripristino anche con soluzioni temporanee (workaround) della funzionalità critica. Tali

backup funzionali devono essere attivabili autonomamente da operatori AUSL o ASMN, opportunamente formati, al più con supporto di INGCLIN o STIT.

- **RP20 –** Il fornitore deve fornire procedure e documentazione scritta necessaria al ripristino dei sistemi e/o le attivazioni dei sistemi di backup funzionale.

2 Requisiti di Rete e Sistemistici

Di seguito sono descritti:

- la configurazione della rete dati, della infrastruttura server e dei client/workstations disponibili presso le aziende AUSL e ASMN
- i requisiti di integrazione di rete e sistemistici

Il fornitore dovrà indicare nella apposita sezione della Scheda Sintetica di Descrizione del Sistema Informativo la rispondenza ai requisiti descritti, motivando eventuali non-conformità. Sempre in tale scheda sarà necessario descrivere le esigenze di connettività del sistema, allo scopo di valutare l'impatto sulla infrastruttura provinciale e predisporre in seguito gli adeguamenti e il supporto necessari.

2.1 Descrizione della infrastruttura aziendale

2.1.1 Infrastruttura di rete

La rete informatica dell'azienda USL di Reggio Emilia è costituita da una rete geografica territoriale distribuita, che collega fra loro sei distretti periferici e le relative 60 sedi, comprendenti servizi amministrativi e sanitari, e sei presidi ospedalieri e un magazzino farmaceutico centralizzato.

Le modalità di interconnessione sono realizzate principalmente su rete Lepida con collegamenti ridondati in fibra ottica o ponte radio per i presidi ospedalieri e linee fibra o rame HDSL/simmetrici con connettività MPLS per le restanti sedi periferiche.

All'interno dei presidi Ospedalieri è presente una rete capillare di distribuzione sia di tipo wired che di tipo wireless, caratterizzata dalla convergenza su almeno un centro stella presente in loco.

La parte wired è realizzata con cavi a coppie UTP di cat.6 o cat.5e, secondo lo standard TIA/EIA 568, e dorsali in fibra ottica monomodale 9-125 con terminazioni SC e multimodale 62,5-125 o 50-125 con terminazioni SC. Tutti gli armadi periferici dello stesso presidio ospedaliero sono collegati con doppio collegamento in fibra con i router della sede ospedaliera.

In particolare la rete LAN è così caratterizzata:

- Presidio Ospedaliero S. Maria - l'architettura di rete è di tipo L3 e ogni armadio periferico prevede una sottorete (subnet) separata e distinta dalle altre con indirizzi di classe C e default gateway distinti. Oltre alla sottorete dedicata ai client aziendali, sono presenti sottoreti separate e segmentate per gli apparati biomedicali, apparati PACS e una rete fisica dedicata per gli apparati di videosorveglianza/tecnici. Gli apparati di rete sono di marca Cisco, con tecnologia di connessione prevalente switched-ethernet a 1Gb/sec in periferia e per le dorsali in fibra ottica dedicata verso i due centri stella, e controllo degli accessi a livello rete tramite sistema NAC.
- Altri presidi Ospedalieri - L'architettura di rete è di tipo L3 suddivisa per ogni presidio ospedaliero, con unico ambito L2 e unica sottorete dei client aziendali su tutti gli armadi periferici del presidio. Oltre alla sottorete dedicata ai client aziendali, sono inoltre presenti sottorete separate e segmentate per gli apparati biomedicali, apparati PACS e di videosorveglianza/tecnici.

Gli apparati di rete sono di marca Extreme Networks, con tecnologia di connessione prevalente switched-ethernet a 100Mbps, con un centro stella nel distretto principale di RE e backup presso il presidio S.Maria per i restanti presidi ospedalieri

La copertura wireless è realizzata secondo lo standard IEEE 802.1a/b/g ed è distribuita su tutti distretti ospedalieri e presso le recenti strutture distrettuali periferiche attraverso gli stessi SSID a livello aziendale.

L'infrastruttura è di tipo centralizzato e costituita da Wireless Control System (WLC) e antenne di marca Cisco, sul presidio ospedaliero S.Maria, e di tipo distribuito con antenne Extreme Networks e controller centrale sui restanti presidi Ospedalieri. L'autenticazione di rete è basata su una tecnologia EAP ovvero WAP2 e la crittografia dati è la AES, con necessità di supporto certificato aziendale per la connettività client. Per i Dispositivi Medici che sfruttino connettività WiFi è prevista una sottorete WiFi dedicata posta fuori dal dominio aziendale, con segmentazione e verifica puntuale degli accessi. Per quest'ultima, l'autenticazione di rete ed encrytion è di tipo WPA2-PSK.

L'unico protocollo di rete ammesso è il TCP/IP. Le connessioni verso l'esterno/Internet avvengono attraverso due coppie di firewall aziendali, che gestiscono tutti le richieste di accesso con opportune regole di filtri e verifiche antivirus/antimalware.

2.1.2 Server

Il parco Server aziendale per gli applicativi clinici è organizzato su diversi DataCenter, posti presso il campus ospedaliero S.Maria, presso il campus S. Lazzaro e presso le strutture Lepida sul territorio regionale.

Come da direttive nazionali, il punto centrale dell'attuale infrastruttura Server dall'azienda USL di Reggio Emila è da identificarsi presso i DataCenter Lepida, identificati come DataCenter primario a Ferrara e come sito di Disaster Recovery su Parma. I DataCenter locali presso le strutture aziendali sono da considerarsi come esclusivo mantenimento dei sistemi cache su applicazioni critiche sanitarie definite.

Presso i Datacenter Lepida, è presente un sistema principale virtuale multinodo VMWare, con replica asincrona delle macchine sul sistema virtuale sul sito secondario. E' inoltre presente sul Datacenter secondario un ambiente di test dedicato, con macchine isolate e non comunicanti con il sistema di produzione.

Questa infrastruttura è collegata alla rete LAN dell'azienda USL tramite doppio collegamento ridondato su rete Lepida e consegnato su percorsi distinti e ridondati nella sede del campus S.Lazzaro e nell'Ospedale S.Maria Nuova.

Il traffico di rete con i client è regolato da appositi firewall per ogni DataCenter gestiti internamente da STIT, che autorizza e verifica il traffico da e verso le reti DataCenter regionali in cui sono collocati i Server applicativi.

I sistemi server aziendali si integrano principalmente in una piattaforma Microsoft costituita da macchine con S.O. MS Windows 2016 e MS Windows 2019 , che prevede i principali servizi infrastrutturali, come MS Active Directory 2012, DHCP, DNS, Management e patching centralizzato

con MS SCOM e MS SCCM 2012, Antivirus Server Microsoft SCEP 2012, Web Application MS IIS 7.0 e successivi e SharePoint 2013.

Sono inoltre disponibili sistemi di gestione e macchine in ambito OpenSource, con sistemi CentoOS, RedHat e OracleLinux.

I database degli applicativi aziendali, principalmente di ambito clinico, sono di tipo MS SQL 2017 o successivi , sia di tipo Oracle Enterprise 12c o successive.

La ridondanza dei sistemi è realizzata con configurazioni HA dei sistemi virtuali, bilanciamento applicativo con sistemi appositi (KEMP, Netscaler) o cluster applicativi dedicati.

2.1.3 Client

I PC aziendali standard (client aziendale) sono dotati di immagine aziendale standardizzata con sistema operativo Windows 7 o Windows 10 e utilizzano solo il protocollo di rete TCP/IP. La messa in rete dei dispositivi client è consentita solamente previa accettazione e mantenimento dei requisiti minimi di sicurezza necessari e con applicazione di policy di dominio aziendale specifiche, alcune delle quali non escludibili.

Il parco client aziendale ha caratteristiche hardware differenti, con processore da I3-4generazione e 4 GB di RAM a processore I3-10generazione e 8/16GB di RAM.

Gli applicativi standard installati sono: agente Microsoft SCCM 2012, Antivirus TrendMicro ApexOne 2019, Suite di produttività Microsoft Office 2016 o M365 Office2016, framework 4.7 e successivi.

I browser generalmente installati sui client sono Chrome aggiornato alle ultime versione e IE11-ultima versione (in corso di dismissione).

2.2 Requisiti di Integrazione Server e Client

Gli scenari di integrazione server e client proposti (e quindi unici ammissibili) per lo specifico sistema informativo sono indicati nella Scheda di Integrazione.

In questo documento, di seguito, sono descritti i requisiti specifici previsti da ciascuno scenario possibile.

Si ritengono impliciti (ma oggetto a verifica) i requisiti di compatibilità elettrica e di rete con le reti di alimentazione e dati presenti nelle aziende.

2.2.1 Server

Server in Fornitura

Il sistema può prevedere la fornitura autonoma di sistemi hardware per le componenti server.

- **RS1.** In tale scenario i server previsti si dovranno collocare presso le sale server aziendali del presidio ospedaliera S.Maria in modalità rack, previa dichiarazione del fornitore di necessità di server ospitato in locale.

Appoggio su Servers Aziendali

Il sistema può, qualora non sia prevista la fornitura autonoma di sistemi hardware, appoggiarsi sulla infrastruttura server virtualizzata e storage enterprise resa disponibile dall'azienda USL di Reggio Emilia per i sistemi clinici presso di DataCenter Lepida.

- **RS2.** Qualora fosse previsto di appoggiarsi sull'infrastruttura server aziendale, questa prevede unicamente i seguenti ambienti virtualizzati e cluster DB :
    - Sistema con infrastruttura VMWare 6.5 o successive ed installazione dei VMWare tools sulle macchine
    - DBMS Oracle 12g o Microsoft SQL Always On 2017
    - Compatibilità del sistema con Microsoft SCEP 2012 o successivi per macchine Windows

L'infrastruttura di storage aziendale disponibile presso di DataCenter Lepida prevede diversi tagli di Storage Base o prestazionale su sistema SAN, e sistema storage NAS scale-out NSF o CIFS.

Qualora fosse previsto di appoggiarsi sull' infrastruttura server aziendale, è necessario che in Scheda Sintetica di Descrizione del Sistema Informativo siano fornite le caratteristiche delle macchine server se proposte in modalità virtuale, ed una analisi di dimensionamento dello storage e delle prestazioni necessarie per anni 2 dalla attivazione del sistema.

Gestione Sistemistica dei Server

- **RS3.** La gestione della parte server (aggiornamento S.O., patching, fixing ecc.), sia offerta in modalità fisica o virtualizzata, rimane totalmente a carico del fornitore, mentre può essere richiesta allo STIT la gestione dell'antivirus aziendale sui server del sistema offerto, purché il fornitore dichiari la compatibilità dell'antivirus aziendale (Microsoft SCEP 2012) col sistema server proposto.

Backup Dati

Il sistema deve prevedere un sistema di backup dati (requisito già incluso tra quelli minimi di sicurezza). Tale sistema di backup dati può essere autonomo, o appoggiarsi sui sistemi di backup aziendale.

- **RS4.** Qualora applicabile, il sistema informativo si può appoggiare sul backup aziendale tramite:
    - Installazione di apposito agent per la protezione del DB dati o appoggio sulla farm aziendale
    - Snapshot giornaliera delle macchine virtuali, con agent sul sistema di virtualizzazione
    - Trasferimento periodico dei files dati verso spazi condivisi di rete soggetti a backup aziendale od utilizzo di libreria DDBoost per salvataggio in apposita appliance di backup
- **RS5.** Se ci si avvale di sistema di backup autonomo da quello aziendale, Il sistema deve prevedere strumenti di reportistica/monitoraggio sulla corretta esecuzione del backup e prevedere invio periodico degli stessi.

AntiVirus

Per ogni server incluso in fornitura deve essere compreso un sistema di gestione antivirus/antimalware. Tale antivirus può essere oggetto della fornitura, o essere mutuato dalla infrastruttura aziendale ASMN.

Qualora compreso nella fornitura:

- **RS6.** Il sistema antivirus deve prevedere aggiornamento automatico delle firme / configurazioni (tramite linea dati in fornitura o passaggio attraverso il SIO) e deve ove possibile essere attivata la protezione real-time dello stesso.

- **RS7.** Il sistema antivirus deve prevedere console di verifica dello stato di aggiornamento e dello stato di tutte le macchine poste sotto copertura, oltre all'invio di dati periodici di allarme e/o rilevazione virus

Il sistema antivirus (in fornitura o aziendale) potrà essere configurato secondo le modalità ritenute più consone alla funzione di ciascun server, nel rispetto delle Misure Minime di Sicurezza ICT vigenti.

2.2.2 Client

Clients in Fornitura

Il sistema può prevedere la fornitura autonoma di client.

In questo caso sono previsti i seguenti requisiti:

- **RS8.** Il client deve prevedere la connessione (join) verso il Dominio aziendale di competenza (gestito tramite controllers Microsoft Active Directory). Qualora non fosse possibile la connessione verso il Dominio è necessario documentarne il motivo in Scheda Sintetica di Descrizione del Sistema Informativo.
- **RS9.** Il client in fornitura per essere messo in rete deve essere in supporto diretto del produttore del sistema operativo, in modo da ricevere patch di sicurezza e di gestione delle vulnerabilità. Non sarà consentito la connessione in rete di dispositivi obsoleti o fuori main-stream support (eg. Client XP o Win7).

Appoggio su Client Aziendali

- **RS10.** Eseguibili: eventuali applicativi da installare o eseguire su client aziendali devono essere files eseguibili a 32 bit o 64bit.
- **RS11.** Setup: il setup della installazione dell'applicativo deve essere in tecnologia MSI Windows Installer.
- **RS12.** Collocazione applicativi su file system client aziendali: I componenti (eseguibili, DLL o altro) delle applicazioni devono essere installati in %ProgramFiles%\<nome azienda>\<nome applicazione> se non sono condivisi. Se devono essere condivisi da altri applicativi in: directory file comuni\<nome società> o %ProgramFiles%\<nome fornitore>\File condivisi.
- **RS13.** Versione e Release: per ogni applicativo software offerto deve essere chiaramente indicato il numero di versione e release, e deve esserne data comunicazione al referente informatico per analisi e catalogazione

Backup Funzionale

- **RS13.**Per ogni client/workstation che svolga ruolo critico per la continuità funzionale del sistema, e che preveda l'archiviazione locale di dati di configurazione necessari al suo funzionamento deve essere previsto un sistema di backup di tali dati, autonomo o appoggiato sui sistemi di backup aziendali (in questo caso tramite copia dei files di interesse in apposito spazio oggetto di backup aziendale).

AntiVirus

Per ogni client previsto in fornitura deve essere compreso un sistema di gestione antivirus. Tale antivirus può essere oggetto della fornitura, o essere mutuato dalla infrastruttura aziendale ASMN.

Qualora compreso nella fornitura:

- **RS14.** Il sistema antivirus deve prevedere aggiornamento automatico delle firme / configurazioni (tramite linea dati in fornitura o passaggio attraverso il SIO) e deve ove possibile essere attivata la protezione real-time dello stesso.
- **RS15.** Il sistema antivirus deve prevedere console di verifica dello stato di aggiornamento e dello stato di tutte le macchine poste sotto copertura, oltre all'invio di dati periodici di allarme e/o rilevazione virus

Il sistema antivirus (in fornitura o aziendale) potrà essere configurato secondo le modalità ritenute più consone alla funzione di ciascun client/workstation, nel rispetto delle Misure Minime di Sicurezza ICT vigenti.

3 Requisiti di Integrazione coi principali componenti del Sistema Informativo Sanitario provinciale

Di seguito è descritto l'insieme delle integrazioni possibili coi principali componenti del sistema informativo sanitario provinciale.

Le integrazione previste per lo specifico sistema informativo (che costituiscono requisiti) sono indicati nella Scheda di Integrazione.

Il fornitore dovrà indicare nella apposita sezione della Scheda Sintetica di Descrizione del Sistema Informativo la rispondenza ai requisiti di integrazione, ritenendo vincolanti quelli indicati in Scheda di Integrazione e facoltativi quelli non indicati in tale scheda.

Nella implementazione delle integrazioni si considera come parte della fornitura (quindi a carico dell'offerente da prevedere in offerta qualora ci si trovi in fase di gara/acquisizione) ogni attività di configurazione da parte del fornitore stesso o fornitore dei sistemi aziendali coinvolti, o altro fornitore terzo coinvolto per le attività di sviluppo, configurazione o installazione delle integrazioni. Nessun onere aggiuntivo rispetto a quanto previsto in fornitura potrà essere

3.1 Integrazioni con la Dorsale Interoperabile

Per una descrizione dettagliata delle integrazioni con la Dorsale Interoperabile, fare riferimento all'Allegato X.1 (Integrazione con la Dorsale Interoperabile (DI))

- **RI1.** Qualora il sistema informativo gestisca dati nominali di assisti/pazienti è necessario integrarlo con l'anagrafe provinciale (SAC).
- **RI2.** Qualora il sistema informativo preveda la generazione di dati sanitari (referti o altro), è necessario integrarlo con il repository provinciale (DWH) per la pubblicazione elettronica dei dati.
- **RI3.** Qualora il sistema informativo preveda l'utilizzo di dati sanitari provenienti da altri sistemi informativi (es. esiti di laboratorio analisi, referti radiologici, ecc.) è necessario integrarlo con il repository provinciale (DWH) per il recupero elettronico dei dati.

- **RI4.** Qualora il sistema informativo preveda l'invio di richieste di accertamento / prestazione verso altri sistemi (es. richiesta di esami di laboratorio, accertamenti radiologici, consulenze) è necessario integrarlo con il sistema di order entry provinciale (OE) per la trasmissione degli ordini
- **RI5.** Qualora il sistema informativo si ponga come sistema di ricezione di richieste di accertamento / prestazione provenienti da altri sistemi (es. sistema di refertazione ambulatoriale o refertazione consulenze) è necessario integrarlo con il sistema di order entry provinciale (OE) per la ricezione degli ordini

3.2 Integrazione con i Sistemi Informativi Amministrativi

Per documenti di specifiche relativi ai sistemi citati, rivolgersi allo STIT.

- **RI6.** Qualora il sistema informativo preveda la rilevazione di prestazioni erogate oggetto di rendicontazione economica, è necessario integrarlo con il Repository Amministrativo (HUB)
- **RI7.** Qualora il sistema preveda la gestione di attività erogate in regime ambulatoriale con obbligo di calcolo ticket è necessario integrarlo con il sistema di Servizio Cassa (CAES)
- **RI8.** Qualora il sistema preveda la Firma Digitale e la conseguente generazione di documenti firmati digitalmente (formato PADES e CADES) è necessario integrare il sistema per l'invio in conservazione sostitutiva (sistema concentratore Biblos, che invia su Polo Archivistico Regionale PARER)

3.3 Altre Integrazioni

Per documenti di specifiche relativi ai sistemi citati, rivolgersi allo STIT.

- **RI9.** Qualora il sistema prevede la generazione, insieme alla componente documentale (per cui sussiste il requisito di invio al repository, vedi punti precedenti), anche di componente iconografica, multimediale o tracciato dati di interesse per la consultazione da parte di operatori sanitari esterni all'unità operativa che ha in uso il sistema, è necessario prevedere l'integrazione verso l'Archivio Immagini Extra-Radiologico (VNA)

4 Requisiti Aggiuntivi

- **RA1.** Qualora il sistema preveda funzionalità di firma digitale devono essere previsti servizi di fornitura SmartCard ed ogni servizio necessario a garantire la continuità operativa (es. procedure di emissione smart card di emergenza in caso di smarrimento o malfunzionamento).
- **RA2.** Qualora previsto da contratto un sistema di tele-monitoraggio o di tele-assistenza sul sistema informativo, questo deve essere in modo non vincolato dalla disponibilità di connettività di rete aziendale, appoggiandosi su connessioni dati autonome comprese in fornitura. L'eventuale assenza di connettività di rete aziendale non può infatti in alcun caso essere giustificazione per l'interruzione dei servizi di tele-monitoraggio e tele-assistenza contrattualmente previsti.

5 Collaudo

Il collaudo del sistema informativo, condotto dallo STIT (congiuntamente con INGCLIN qualora siano coinvolti dispositivi medici o forniture di competenza di questo servizio), prevede:

- L'accettazione formale da parte di ASMN e/o AUSL delle dichiarazioni di conformità (di cui la Scheda Sintetica di Descrizione del Sistema Informativo è parte integrante)
- L'accettazione formale da parte di ASMN e/o AUSL di ogni deroga ai requisiti sopra esposti, a seguito di motivazione documentata

- La verifica tecnica del corretto funzionamento di ogni integrazione prevista nella Scheda di Integrazione

Il collaudo è da intendersi come step formale obbligatorio per la messa in produzione del sistema, ma non esime il fornitore dal rispetto dei requisiti e delle garanzie di corretto funzionamento per il resto del periodo contrattuale, come regolamentato nello specifico dallo specifico contratto di acquisizione (o come descritto in Capitolato).

Il collaudo positivo, a meno di indicazioni contrattuali specifiche, è vincolante per ogni attività di fatturazione da parte del fornitore del sistema software nei confronti di ASMN e/o AUSL.

6 Allegati

Allegato X.0 – Scheda di Integrazione (opzionale)

Allegato X.1 – Integrazione con la Dorsale Interoperabile (DI)

Allegato X.9 – Scheda Sintetica di Descrizione del Sistema Informativo (obbligatorio se presente Allegato X.0)