AS FO
Azienda sanitaria
Friuli Occidentale

REGIONE AUTONOMA FRIULI VENEZIA GIULIA

DETERMINAZIONE

del Dirigente Responsabile

APPROVVIGIONAMENTI E GESTIONE CONTRATTI BENI E SERVIZI

N. 145 DEL 11/02/2026

OGGETTO

Gara a procedura aperta, ai sensi dell'art. 71 del D.Lgs. n. 36/2023 e ss.mm. e ii., per la conclusione di un accordo quadro, suddiviso in quattro lotti, finalizzato alla fornitura di impianti cocleari e protesi acustiche impiantabili ed eventuale fornitura di componenti sostitutive per le parti usurabili degli impianti in favore dell'Azienda Sanitaria Friuli Occidentale. Approvazione chiarimenti e documentazione integrativa.

Oggetto: Gara a procedura aperta, ai sensi dell'art. 71 del D.Lgs. n. 36/2023 e ss.mm. e ii., per la conclusione di un accordo quadro, suddiviso in quattro lotti, finalizzato alla fornitura di impianti cocleari e protesi acustiche impiantabili ed eventuale fornitura di componenti sostitutive per le parti usurabili degli impianti in favore dell'Azienda Sanitaria Friuli Occidentale. Approvazione chiarimenti e documentazione integrativa.

IL DIRIGENTE RESPONSABILE APPROVVIGIONAMENTI E GESTIONE CONTRATTI BENI E SERVIZI

Normativa di riferimento:

RICHIAMATE le seguenti disposizioni:

- Legge regionale n. 17 del 16/10/2014 recante "*Riordino dell'assetto istituzionale e organizzativo del Servizio Sanitario regionale e norme in materia di programmazione sanitaria e sociosanitario"*, come da ultimo modificata dalla legge regionale n. 27 del 17/12/2018 recante *"Assetto istituzionale e organizzativo del Servizio Sanitario regionale"*;
- DGR n. 2174 del 12/12/2019 recante "*L.R. 27/2018, art. 3 e art. 11: assetto del servizio sanitario regionale – Costituzione dei nuovi Enti*", con la quale è stata, tra l'altro, disposta la modifica della denominazione dell'Azienda per l'Assistenza Sanitaria n. 5 "Friuli Occidentale" (AAS5) con sede legale a Pordenone, in Azienda sanitaria Friuli Occidentale (AS FO) a far data dall'1/01/2020;
- Decreto del Presidente della Regione Friuli Venezia Giulia n. 0223 del 20/12/2019, con cui è stata data attuazione alla succitata DGR 2174/2019;
- Decreto del Direttore Generale n. 474 del 01/06/2022 di adozione, in via definitiva, dell'Atto Aziendale, decreto n. 939 del 07/11/2022 di revisione dell'organigramma e decreto n. 132 del 10/02/2023 recante "*Atto Aziendale: seconda revisione organigramma*";
- Art. 22 dell'Atto Aziendale – allegato da ultimo al decreto n. 132 del 10/02/2023 sopra citato – per la disciplina delle competenze dirigenziali;
- Allegato A all'Atto Aziendale (*Organigramma Aziendale*);
- Decreto del Direttore Generale n. 650 del 07/08/2023 di "*Applicazione Atto aziendale di cui al decreto n. 132 del 10/02/2023. Dipartimento Amministrativo: determinazioni.*";
- Decreto del Direttore Generale n. 688 del 21/08/2023, rubricato "*Applicazione Atto Aziendale di cui al decreto n. 132/2023: ricognizione attività e determinazioni conseguenti. Prima fase*";
- Decreto del Diretto Generale n. 713 del 12/09/2023 "*Parziale rettifica decreto n. 650 del 07/08/2023 recante "Applicazione Atto aziendale di cui al decreto n. 132 del 10/02/2023. Dipartimento Amministrativo: determinazioni"*.
- Delibera della Giunta regionale n. 1507 del 31/10/2025, avente ad oggetto *"LR 22/2019, art. 50. Linee annuali per la gestione del Servizio Sanitario Regionale per l'anno 2026. Approvazione definitiva. Finanziamento agli Enti del S.S.R. per l'anno 2026 - Assegnazione e erogazione in via provvisoria*";
- il Decreto del Direttore Generale n. 1106 del 23/12/2025 *"Piano Attuativo e Bilancio Preventivo 2026. Adozione definitiva"*;
- - il Decreto del Direttore Generale n. 13 del 09/01/2026 *"Assegnazione dei Budget di Risorsa per l'anno 2026"*;
- Decreto del Direttore Generale n. 656 del 14/07/2021 di conferimento di Direttore della S.C. Approvvigionamenti e gestione contratti beni e servizi;

- Decreto del Direttore Generale n. 526 del 24/06/2022 di adozione del Regolamento di utilizzo dell'identità visiva dell'Azienda sanitaria Friuli Occidentale;
- Decreto Legislativo n. 36 del 31/03/2023 s.m.i., "*Codice dei contratti pubblici in attuazione dell'articolo 1 della legge 21 giugno 2022, n. 78 recante delega al Governo in materia di contratti pubblici*";
- Allegato I.2 al Decreto Legislativo n. 36 del 31/03/2023 recante "*Attività del RUP*";
- Decreto del Direttore Generale n. 460 del 14/06/2024 di "*Approvazione Regolamento aziendale per la determinazione e ripartizione degli incentivi per lo svolgimento di funzioni tecniche ai senti dell'art. 45 D.Lgs. 36/2023.";*
- Decreto del Direttore Generale n. 539 del 19/06/2025, recante "*Programmazione triennale degli acquisti di beni e servizi ai sensi dell'art. 37 del D.Lgs. 36/2023. Approvazione programma triennale 2025-2026-2027 e aggiornamento Programma triennale degli acquisti di beni e servizi di importo unitario stimato superiore a 1 Milione di euro per gli anni 2025-2026-2027*".

Istruttoria e motivazione dell'atto:

PREMESSO che, con determinazione n. 37 del 19/01/2026, è stata indetta la gara a procedura aperta ai sensi dell'art. 71 del D.Lgs. n. 36/2023 e ss.mm. e ii. per la conclusione di un accordo quadro, suddiviso in quattro lotti, finalizzato alla fornitura di impianti cocleari e protesi acustiche impiantabili ed eventuale fornitura di componenti sostitutive per le parti usurabili degli impianti in favore dell'Azienda Sanitaria Friuli Occidentale;

DATO ATTO che, entro i termini stabiliti nel bando di gara, sono pervenute delle richieste di chiarimenti presentate da alcuni operatori interessati a partecipare alla procedura in oggetto;

PRESO ATTO che, a seguito della ricezione delle richieste di cui sopra, è stata rilevata l'opportunità di chiarire e integrare alcuni elementi già presenti nella documentazione della gara in oggetto al fine di garantire i principi di trasparenza, di libera concorrenza e di parità di trattamento di cui al D.Lgs. 36/2023 e ss.mm. e ii.;

RILEVATO in particolare che le risposte alle richieste di chiarimenti sono state pubblicate nell'area pubblica della piattaforma eAppaltiFVG e nella Sezione "Amministrazione Trasparente" del sito aziendale, all'indirizzo *https://asfo.sanita.fvg.it/it/bandi-gara/*;

RITENUTO per quanto sopra esposto di procedere:
- all'approvazione integrale degli allegati al presente atto, ad integrazione di quelli già approvati con determinazione n. 37 del 19/01/2026 cit.;
- alla modifica del bando di gara approvato con determinazione n. 37 del 19/01/2026 cit.;

DATO ATTO che sarà disposta la pubblicazione del presente provvedimento su:
- piattaforma eAppaltiFVG;
- sito aziendale *https://asfo.sanita.fvg.it/it/bandi-gara/*;

Attestazione di compatibilità dell'atto rispetto al bilancio economico di previsione:

SI ATTESTA che dal presente atto non derivano costi a carico del bilancio aziendale di competenza;

VISTO:

- l'allegato A all'Atto Aziendale (Elenco dei dipartimenti e delle strutture aziendali complesse e semplici di dipartimento), in cui sono indicati il mandato e le funzioni di questa Struttura;
- il Decreto del Direttore Generale n. 1106 del 23/12/2025 *"Piano Attuativo e Bilancio Preventivo 2026. Adozione definitiva"*;
- il Decreto del Direttore Generale n. 13 del 09/01/2026 *"Assegnazione dei Budget di Risorsa per l'anno 2026"*;

- DETERMINA -

per i motivi di cui in premessa, che si intendono integralmente riportati:

1. di procedere all'integrazione della documentazione di gara della procedura indetta con determinazione n. 37 del 19/01/2026, così come indicato negli allegati al presente provvedimento, parti integranti e sostanziali dello stesso;

2. di dare atto che il termine stabilito per gli operatori economici per avanzare richiesta di chiarimenti, già fissato al 09/02/2026, è definitivamente spirato;

3. di dare atto che rimane invariata ogni altra condizione di gara, tra cui requisiti di partecipazione, CIG, prezzi a base d'asta e importo della garanzia provvisoria;

4. di disporre la pubblicazione del presente provvedimento su:
   - piattaforma eAppaltiFVG;
   - sito aziendale https://asfo.sanita.fvg.it/it/bandi-gara/;

5. di dare atto, altresì, che il RUP è il Direttore della S.C. Approvvigionamenti e gestione contratti beni e servizi;

6. di riservarsi di adottare gli atti propedeuticamente necessari a dare attuazione al presente provvedimento;

7. di dare atto che il presente provvedimento è soggetto agli obblighi di pubblicità e trasparenza di cui all'art. 37 del D.Lgs. 14 marzo 2013 n. 33 e che non si rilevano conflitti di interesse in riferimento al presente provvedimento;

8. di prendere atto che sarà cura della Struttura proponente comunicare gli esiti di tale provvedimento ai Servizi utilizzatori interessati, tramite la funzione "predisposizione notifiche", prevista dall'applicativo aziendale in uso per l'adozione degli atti deliberativi;

9. di dare atto, infine, che il presente provvedimento è immediatamente esecutivo in relazione a quanto previsto dall'art. 4 comma 2 L.R. 21/1992 e ss.mm.ii..
10.

Il Dirigente Responsabile - APPROVVIGIONAMENTI E GESTIONE CONTRATTI BENI E SERVIZI
dott.ssa Vania Costella
firmato digitalmente

Elenco allegati:

1	Specifiche IT ASFO-REV0.5 con allegati.pdf
2	Riscontro chiarimenti.pdf
3	MDS2.pdf

Elenco firmatari

ATTO SOTTOSCRITTO DIGITALMENTE AI SENSI DEL D.P.R. 445/2000 E DEL D.LGS. 82/2005 E SUCCESSIVE MODIFICHE E INTEGRAZIONI

Questo documento è stato firmato da:

NOME: VANIA COSTELLA
CODICE FISCALE: CSTVNA67S67Z133O
DATA FIRMA: 11/02/2026 16:34:12
IMPRONTA: A0E9881769190EA4E30394AC76AE3EB9B4A6A22CF2535EA0DD98159509658AEA
B4A6A22CF2535EA0DD98159509658AEA74F998FFB187E040FF62E491EA9FBCE4
74F998FFB187E040FF62E491EA9FBCE409B3C17B6A17F42C04072A4E8C27CA70
09B3C17B6A17F42C04072A4E8C27CA7060CE7944CC2E5026DC8D9E5FBC32B959

S. C. Approvvigionamenti e gestione contratti beni e servizi

Responsabile del procedimento:
Costella dr.ssa Vania

AS FO
Azienda sanitaria
Friuli Occidentale

REGIONE AUTONOMA FRIULI VENEZIA GIULIA

via della Vecchia Ceramica, 1 - 33170 Pordenone (PN) - Italy
C.F. e P.I. 01772890933 PEC: asfo.protgen@certsanita.fvg.it

Pordenone, 10 febbraio 2026

Cartella di gara: tender_81963
Piattaforma eAppaltiFVG

Gara a procedura aperta, ai sensi dell'art. 71 D.Lgs. 36/2023, per la conclusione di un accordo quadro, suddiviso in quattro lotti, finalizzato alla fornitura di impianti cocleari e protesi acustiche impiantabili ed eventuale fornitura di componenti sostitutive per le parti usurabili degli impianti in favore dell'Azienda sanitaria Friuli Occidentale, per 36 mesi.

Con la presente, si dà riscontro alle richieste di chiarimenti pervenute in merito alla cartella di gara: tender_81963:

Quesito n. 1:

Si osserva che la base d'asta per ciascun singolo sistema di soli € 6.000,00 non trova riscontro né con il prezzo di listino (€11.050,00 che comprende : parte impiantabile, elemento protesico "accoppiatore", esoprotesi) né con le aggiudicazioni ottenute presso altre P.A.: si invita a verificare la documentazione allegata che riporta l'aggiudicazione ottenuta per il lotto 7 nella procedura aperta con modalità telematica costituita da sette lotti, della fornitura quadriennale con la formula dell'accordo quadro, di protesi acustiche per le esigenze dell'Azienda Ospedaliero Universitaria di Ferrara e dell'Azienda Ospedaliero Universitaria di Bologna", dalla quale si può evincere chiaramente un prezzo di vendita aggiudicato di € 9.900,00 cad. .
Inoltre si evidenzia come sia stato posto un prezzo a base d'asta per un sistema uditivo ATTIVO addirittura inferiore a quello per un sistema PASSIVO, ovvero inferiore al prezzo di 6.500,00 cad. per il lotto 3.
A fronte di quanto esposto, qualora la base d'asta non venisse aumentata in misura idonea al valore del dispositivo, ci troveremo nella difficile posizione di non presentare offerta per questo lotto che con ogni probabilità, andrà pertanto deserto.

Riscontro:

Dalle informazioni in nostro possesso la base d'asta risulta adeguata.

Quesito n. 2:

Nel disciplinare, a pag. 11 e 12, per i 4 lotti è indicato: "Importo ricambi della componente esterna (5% sulla base d'asta + opzioni)".
In questi importi sono incluse le sostituzioni integrali di esoprotesi?

Riscontro:

Si conferma. Cfr. p. 6.8 del capitolato speciale d'appalto, ultimo capoverso.

Quesito n. 3:

Nel Capitolato speciale, pag. 5, art. 5, è indicato: "L'offerente dovrà compilare e sottoscrivere il modulo di Manufacturer Disclosure Statement for Medical Device Security (MDS2) versione 19, in maniera da permettere ad ASFO una più agevole valutazione delle eventuali criticità della messa in uso dei sistemi offerti anche secondo EC/TR 80001-2-2".
Dove possiamo trovare questo modulo?
Bisogna allegarlo all'offerta tecnica oppure sarà da sottoscrivere insieme alla nomina RTD?

Riscontro:

Il modulo MDS2 è reperibile sul sito del Nema.
Qualora ci fossero difficoltà nell'accesso al sito, si mette a disposizione nell'area allegati dell'RDO di qualifica una versione del documento che richiede gli stessi dati. Lo stesso dovrà essere allegato all'offerta tecnica.

Quesito n. 4:

Inoltre sempre all'art.5 è indicato: "Dal punto di vista della sicurezza, i sistemi dovranno rispondere a quanto richiesto ..... dall'allegato Specifiche IT che è parte integrante del presente documento e il suo contenuto è da considerarsi prevalente rispetto ad ogni altra specifica IT."
A quale allegato si fa riferimento?

Riscontro:

Si mette a disposizione nell'area allegati dell'RDO di qualifica l'allegato *"Specifiche IT".*

Quesito n. 5:

Come da disciplinare, anche sulla piattaforma eappalti è visibile la richiesta di caricamento del DGUE sia in formato pdf che in formato xml.
Tuttavia, non è a noi visibile tra la documentazione di gara allegata sulla piattaforma il file DGUE request in xml necessario alla compilazione del file DGUE response in xml.
Sarebbe possibile ottenere il file?

Riscontro:

Il formato .xml del DGUE è scaricabile dalla piattaforma eAppaltiFVG una volta completato l'inserimento dei dati all'interno del format ESPD. Qualora sussistano delle difficoltà, si invita a contattare il servizio clienti della piattaforma nelle modalità prescritte dal disciplinare di gara al paragrafo 1.3.

Quesito n. 6:

Sulla piattaforma viene richiesto, nella busta amministrativa, il caricamento di una "Dichiarazione di impegno di un fideiussore".
Tuttavia, nella sezione dedicata alla garanzia provvisoria non viene specificata la natura dell'impegno che il fideiussore dovrebbe assumersi.
Potete confermare se con ciò si intende semplicemente l'impegno espresso del garante a rinnovare la garanzia ai sensi dell'articolo 106, comma 5 del Codice, su richiesta della stazione appaltante per ulteriori 180 giorni, oppure se viene richiesta la dichiarazione di commitment del garante ad emettere la garanzia definitiva?
Si fa notare che tale commitment non è più necessario ai fini della legge, e nel caso venisse espressamente richiesto dalla stazione appaltante, sarebbe da chiarire anche la misura nella quale questo viene richiesto.

Riscontro:

Si conferma che è richiesta la dichiarazione di impegno del garante a rinnovare la garanzia ai sensi dell'articolo 106, comma 5 del Codice, su richiesta della stazione appaltante per ulteriori 180 giorni, nel caso in cui al momento della sua scadenza non sia ancora intervenuta l'aggiudicazione.

Quesito n. 7:

Buonasera, siamo cortesemente a richiedere il seguente chiarimento in rif. all'art. 6.8 Assistenza tecnica. "L'O.E. dovrà garantire sul territorio di riferimento AS FO almeno un centro con personale specializzato per l'assistenza tecnica e sostituzione di componenti usurati o difettosi sulla parte esterna dei dispositivi impiantati. I collaboratori sul territorio, se non sono dipendenti dell'O.E., verranno qualificati quali subappaltatori salvo la presentazione di accordi continuativi di cooperazione da parte dell'O.E. aggiudicatario".
Dato che per l'assistenza tecnica abbiamo in atto dei contratti di concessione con dei centri autorizzati, ci confermate che sarà sufficiente presentare i suddetti contratti, senza doverci avvalere di ulteriori contratti di subappalto?
In caso contrario, cosa si intende con: "salvo la presentazione di accordi continuativi di cooperazione da parte dell'O.E. aggiudicatario"?
Grazie.

Riscontro:

Si conferma che è sufficiente presentare i contratti in questione.

Si coglie l'occasione per ricordare che il 09/02/2026, alle ore 23:59, è scaduto il termine per la presentazione delle richieste di chiarimenti, pertanto ulteriori quesiti pervenuti dopo tale data non potranno essere evasi.

Distinti saluti.

Il Direttore
S.C. Approvvigionamenti e
gestione contratti beni e servizi
- *Costella dr.ssa Vania* -

Allegato specifiche IT Medicali e Analitici AsFO

Introduzione

Il presente documento ha come scopo regolamentare, tramite informazione e categorizzazione in casi d'uso, l'ingresso dei nuovi sistemi forniti in qualsivoglia modalità (acquisto, noleggio, service, donazione, …).

La parte informativa del documento rappresenta le specifiche che i sistemi/beni forniti dovranno rispettare relativamente all'area IT. Nel documento verrà fornita una panoramica che riporterà concetti fondamentali sulla tipologia di rete presente in AsFO e le metodologie legate all'integrazione dei sistemi offerti con quelli esistenti.

La categorizzazione dei casi d'uso viene definita in coerenza con la legislazione vigente, normativa generale e specifica di settore, linee guida e best practice, sempre e comunque a tutela di AsFO, nell'interesse dell'Azienda e dei fruitori dei servizi erogati. Casi d'uso non riconducibili alla categorizzazione presentata dovranno essere analizzati e validati prima dell'affidamento del contratto.

In nessun modo elementi indicati nell'offerta tecnica da parte del fornitore, in contrasto con quanto riportato nel presente documento, avranno valenza contrattuale.

Resta inteso che dovrà essere fornito tutto il supporto necessario dal fornitore e tutta la documentazione utile riguardante i sistemi forniti per consentire ad AsFO di rispondere a tutte le indicazioni rappresentate nella governance nazionale vigente per l'area di riferimento.

Normativa e tecnica di riferimento

Privacy: corrispondenza dei sistemi e beni a quanto indicato - dal Regolamento Europeo sulla Protezione dei Dati – GDPR del 14.04.2016 (https://eur-lex.europa.eu/) e al D. Lgs. 196/2003 s.m.i., cosiddetto Codice Privacy, così come novellato dal d.lgs. 101/2018; l'aggiudicatario verrà designato responsabile ex art.28 del GDPR e dovrà produrre ed attuare tutto quanto richiesto, per quanto pertinente prima del collaudo e per tutta la durata del contratto.

Cybersecurity-cloud: corrispondenza di quanto fornito alla Circolare AGID 18 aprile 2017, n. 2/2017, recante "Misure minime di sicurezza ICT per le pubbliche amministrazioni", con livello ALTO; inoltre l'aggiudicatario dovrà collaborare attivamente per quanto oggetto di fornitura alla produzione di documentazione che l'AsFO è chiamata a redigere in ottemperanza alla suddetta circolare AGID.

In riferimento allo sviluppo e all'acquisizione di software dovranno essere rispettate le indicazioni di AgID secondo quanto riportato nelle "linee guida di sicurezza nello sviluppo delle applicazioni". Dovrà essere garantita la conformità alle regole sull'interoperabilità prescritte dalle linee guida emanate in attuazione dell'art. 73 del CAD.

Dovrà essere possibile per AsFO esportare l'intera base di dati (inclusi di ogni tipo di indice o metadato utilizzato per implementare le funzionalità del software stesso) in formato standard e

aperto, per scongiurare la possibilità di lock-in, come meglio specificato nelle linee guida n.8 di ANAC.
Il fornitore si renderà disponibile a produrre il dettaglio del oggetto di fornitura per permettere ad AsFO di ottemperare a quanto indicato nella Direttiva NIS 2 2022/2555 e il d.lgs 138/2024 di recepimento della direttiva, se necessario, nel decreto legge n.105/2019 "Perimetro Nazionale di Sicurezza Cibernetico" e decreti attuativi.
Nello specifico è richiesta la disponibilità del fornitore per supportare AsFO o suoi delegati nei precorsi di analisi e miglioramento previsti dal Framework Nazionale per la Cybersecurity e Data Protection, ovvero dalla normativa nazionale vigente in materia di cybersecurity.
Disponibilità totale del fornitore a fornire le informazioni necessarie e intraprendere i percorsi per permette ad AsFO di ottemperare a quanto indicato e definito dall'Agenzia per la Cybersicurezza Nazionale (ACN) e dal Dipartimento per la Trasformazione Digitale (DTD) in relazione alla cybersecurity e al cloud.

Requisiti/riferimenti particolari
La rete aziendale di AsFO, in quanto integrante dispositivi e applicazioni individuati come dispositivo medico secondo MDR (e IVDR), e quanto definito all'art.120 del regolamento per il periodo transitorio, si intende come rete IT medicale ai sensi di quanto indicato dalla norma ISO IEC 80001-1.
In conseguenza di ciò si precisa che il collaudo di sistemi (inclusivi di DM e non) sarà condizionato alla redazione e sottoscrizione di un accordo di responsabilità, dove si evidenziano i profili di responsabilità della gestione della fornitura (DRW). Ad esempio la gestione di server virtualizzati, patch OS, dominio, integrazioni e visibilità.
Se l'oggetto di fornitura include dispositivi medici, il fornitore dovrà compilare, sottoscrivere e allegare all'offerta tecnica il modulo Manufacturer Disclosure Statement for Medical Device Security (MDS2) versione 2019 per ciascuno di essi, in maniera da permettere ad AsFO una più agevole valutazione delle eventuali criticità della messa in uso dei sistemi offerti anche secondo EC/TR 80001-2-2. È comunque onere del fornitore verificare la versione più recente del modulo dal sito NEMA e compilare e fornire tale versione.
Inoltre, sempre nel caso in cui l'oggetto di fornitura includa dispositivi medici, il sistema fornito dovrà rispondere a quanto richiesto:
- dal IHE Patient Care Device (PCD) White Paper, "Medical Equipment Management (MEM): Medical Device Cyber Security – Best Practice Guide";
- dalla linea guida "MDCG 2019-16 Guidance on Cybersecurity for medical devices".

In generale l'aggiudicatario si assume la piena responsabilità della sicurezza informatica e del trattamento dei dati affidato nell'ambito di quanto richiesto dalla presente procedura d'acquisto/noleggio/service/donazione, in particolare in merito all'integrità, disponibilità e riservatezza dei dati e dei sistemi. Pertanto, anche nei casi in cui la sicurezza dei dati gestiti dai sistemi oggetto di fornitura possa essere legata agli effetti di altro hardware e software in gestione ad un soggetto terzo, l'aggiudicatario rimane responsabile di monitorare tali elementi e segnalare in via formale qualora ritenga vi siano aspetti di inadeguatezza. In tale responsabilità ricade anche l'onere di richiedere gli strumenti per fare gli audit ed il monitoraggio, per eseguire le ricerche di anomalie, oltre alla comunicazione formale delle proposte percorribili per raggiungere gli obiettivi.
In coerenza con quanto stabilito dal Piano Triennale AGID che suggerisce un approccio "cloud first", i servizi oggetto di fornitura potranno essere erogati in modalità SaaS, aderente nell'erogazione

(tipologia e qualificazione del soggetto erogatore) a quanto indicato dalla Strategia Cloud Italia, fermo restando tutte le prescrizioni riportate nel presente documento. I servizi erogati in modalità SaaS dovranno essere pubblicati sul Cloud Marketplace di ACN, la piattaforma che espone i servizi e le infrastrutture qualificate da ACN secondo quanto disposto nel Decreto direttoriale prot. N. 29 del 02/01/2023.
La soluzione messa a disposizione attraverso l'infrastruttura in cloud dovrà rispettare le caratteristiche previste da ACN e dal regolamento in conseguenza del fatto che verrà utilizzata per l'erogazione di un servizio trattante dati di livello critico secondo la classificazione definita all'interno della Strategia Cloud Italia pubblicata a settembre 2021 dall'Agenzia per la Cybersicurezza Nazionale e il Dipartimento per la Trasformazione digitale.
L'infrastruttura cloud dovrà essere tra quelle qualificate\adeguate di livello pertinente alla tipologia di dati e servizi che vengono trattati su tale infrastruttura secondo quanto indicato nel nuovo Regolamento Cloud di ACN, in vigore dal 1/7/2024, "REGOLAMENTO PER LE INFRASTRUTTURE DIGITALI E PER I SERVIZI CLOUD PER LA PUBBLICA AMMINISTRAZIONE".
Nel caso di acquisizioni di forniture e servizi critici nelle quali nessuno dei partecipanti sia provvisto di adeguata qualificazione\certificazione, AsFO richiede che l'aggiudicatario intraprenda il percorso di certificazione per il livello idoneo. In parallelo AsFO condurrà un analisi del rischio dal punto di vista della sicurezza della soluzione proposta per valutare se il livello di rischio è accettabile per l'avvio del servizio, fermo restando l'impegno dell'aggiudicatario a collaborare attivamente alla stesura della analisi e ad intraprendere il percorso di certificazione da rendere effettivo entro 9 mesi dall'aggiudicazione.

Sarà prevista una fase di test di funzionamento - con la simulazione di interruzioni/guasti- per validare l'affidabilità, la resilienza e la conformità del sistema ai livelli di servizio attesi.
Nel caso la connettività verso il servizio in cloud venga fornita attraverso la rete RUPAR, ritenuta conforme ai requisiti prestazionali richiesti dalla soluzione applicativa - in ottemperanza alla strategia Cloud Italia contenente le indicazioni strategiche per la migrazione dei dati e servizi digitali classificati come critici - il fornitore dovrà garantire la distribuzione dei servizi in cloud (Saas) in alta affidabilità con peering VPC.
I servizi SaaS offerti dovranno essere fruibili tramite collegamento internet invocabile con i web browser in uso presso AsFO e senza alcun componente aggiuntivo sul browser stesso o sul client in generale; la sicurezza delle connessioni tra browser e servizi SaaS remoti dovrà essere adeguata alla tipologia di dati scambiati, in ogni caso dovrà essere adottato il protocollo HTTPS (TLS 1.2 o superiore – in ogni caso non deprecato – con certificato pubblico in gestione e a carico dell'aggiudicatario; tale certificato dovrà essere riconosciuto come valido dai browser di cui sopra, senza specifiche configurazioni, ovvero non dovranno essere usati certificati di tipo self-signed) e in alcun caso verranno realizzate connessioni VPN o di altro tipo ad hoc, per sopperire ad eventuali carenze architetturali in termini di sicurezza o funzionalità, quindi resta inteso che i servizi dovranno sempre essere fruibili in maniera efficace e sicura tramite internet. I server che contengono i dati trattati di titolarità AsFO dovranno risiedere all'interno della UE e per nessuna ragione dovranno essere effettuate copie di tali dati al di fuori del perimetro della UE, neppure per motivi di continuità di servizio e disaster recovery.

Sarà ammessa, e fortemente consigliata, la predisposizione di apparati edge (preferibilimente virtuali, eventualmente su infrastruttura messa a disposizione da AsFO), ovvero server applicativi che possano garantire la piena continuità di servizio in caso di irraggiungibilità del cloud, in un'ottica di applicazione delle best practice di Business Continuity come suggerito dalla norma ISO/IEC 22313:2020. Il server edge dovrà avere ridottissima profondità temporale. Gli apparati di edge

dovranno essere adeguatamente dimensionati (inteso come prestazioni) per l'erogazione di tutti i servizi con la massima efficienza, compresi eventuali servizi di server side rendering necessari all'erogazione dei tool avanzati.

AsFO è responsabile per la sola parte di corretta esecuzione dell'ambiente virtualizzato su cui insistono le macchine virtuali, alimentazione e raffrescamento dei locali tecnici e del collegamento verso la LAN Aziendale, eventualmente verso internet se la connettività verso il sistema in cloud non è provvisto di doppia connessione dedicata fornita dall'aggiudicatario.

Restano in capo all'aggiudicatario la gestione del S.O. della macchina (aggiornamenti e patch di sicurezza), politiche di backup e replica in cloud coerenti con la tipologia di servizio e tutto quanto il necessario alla corretta erogazione del servizio applicativo ad esclusione della connettività alla LAN.

Nel caso in cui l'oggetto di fornitura sia o contenga un software DM è necessario fornire adeguata documentazione da parte del fornitore relativa all'impossibilità di procedere con gli aggiornamenti, di qualsiasi tipo.

Le attività di aggiornamento dovranno essere comunque concordate e documentate nel report DAPS relativo al contratto che verrà stipulato e che lo seguirà lungo tutto il suo periodo di validità.

Qualsiasi malfunzionamento o interruzione del servizio, dovuta al non corretto dimensionamento della infrastruttura è da considerarsi a carico del fornitore.

L'accesso ad Internet (anche cloud del fornitore) delle soluzioni oggetto di fornitura va documentato, validato e attivato solo a seguito della nomina a Responsabile al trattamento del fornitore, su proposta di AsFO.

L'accesso dovrà essere regolamentato come segue:

- autorizzato;
- indicato nel "documento riepilogativo attori e transazioni"
- seguire il principio di minimizzazione dei dati (GDPR);
- solo verso indirizzi specifici;
- solo tramite canali cifrati;
- manutenuto aggiornato.

L'accesso da internet, solamente per scopi manutentivi, alle soluzioni oggetto di fornitura va documentato, validato e attivato solo a seguito della nomina a Responsabile al trattamento del fornitore, su proposta di AsFO.

L'accesso dovrà essere regolamentato come segue:

- autorizzato;
- indicato nel "documento riepilogativo attori e transazioni"
- seguire il principio di minimizzazione dei dati (GDPR);
- solo sulle apparecchiature oggetto di fornitura;
- solo tramite VPN aziendale;
- solo con account nominale;
- possibilmente con MFA.

Con cadenza trimestrale l'aggiudicatario dovrà fornire report degli accessi fatti in VPN per la validazione, indicando: utente, motivazione, attività svolta durata dell'intervento. AsFO potrà in qualsiasi momento richiedere un report anticipato rispetto a quelli programmati per confrontarli con i log del servizio VPN.

Autenticazione applicativa

Relativamente al sistema di autenticazione da utilizzare, dovrà essere possibile attivare nel corso di tutta la durata contrattuale, a discrezione di AsFO e senza oneri aggiuntivi per AsFO stessa, il Single Sign On (SSO), basato sulla piattaforma di interoperabilità, sul quale poggia il sistema di autorizzazione/autenticazione offerto dalla piattaforma di interoperabilità di Insiel che a sua volta si avvale degli endpoint ADFS Aziendali.

Ulteriori requisiti e best practices

Inoltre, sempre in coerenza con quanto stabilito da AGID, i sistemi forniti dovranno essere progettati, realizzati ed installati in modo da minimizzare fenomeni di lock-in e in ogni caso, durante gli ultimi due trimestri di durata del contratto ed eventualmente per i tre mesi successivi, e comunque fino al raggiungimento dell'obiettivo, l'aggiudicatario dovrà favorire in ogni modo il travaso e la fruizione dei dati verso sistemi di terze parti, il che sarà vincolante al pagamento delle ultime due fatture inm caso di servizio, applicazione di penale in caso di singola fornitura. Tali attività ed i servizi professionali e tecnici associati sono perciò da intendersi oggetto di fornitura del presente contratto.
Dovrà essere indicato chiaramente in offerta tecnica in quale contesto tecnologico (client DM/IVD, client Saas ibrido, client Saas con edge così come descritti nel presente documento) ricade l'offerta presentata e dovrà essere dettagliato come - tecnicamente e organizzativamente -l'aggiudicatario intende rispondere alle prescrizioni del presente documento.
In caso di soluzioni rientranti nei contesti 2 e 3 con utilizzo del sistema di virtualizzazione di AsFO come primario o come edge dovrà inoltre essere indicato in offerta tecnica il numero di risorse computazionali richieste (almeno: numero di macchine virtuali, sistema operativo, funzione, RAM, core, spazio disco, necessità in termini di backup e disaster recovery). Se tali richieste dovessero risultare non congrue rispetto alle finalità del contratto o non sostenibili per la stazione appaltante ad insindacabile giudizio di AsFO, AsFO stessa si riserva di richiedere il passaggio alla soluzione SaaS definita nel contesto 3 senza oneri aggiuntivi.
In generale per l'analisi preliminare e l'avviamento all'uso dei sistemi oggetto di fornitura AsFO metterà a disposizione 5 giornate uomo di tecnico sistemista senior e 5 giornate uomo di project manager. La mancanza di autonomia operativa da parte dell'aggiudicatario o particolari necessità di assistenza svolta da personale AsFO, che vadano oltre i limiti sopra riportati, verranno computati da AsFO che si riserva la facoltà di quantificare le relative spese in base al listino allegato alla Convenzione Consip attiva con a listino il servizio necessario o più aderente, e di dedurle dal piano di fatturazione previsto. Con la partecipazione alla gara si intende accettato tale meccanismo compensativo.
Nel caso in cui il sistema fornito, indipendentemente dal contesto di mesa in servizio in cui si trovi, debba integrarsi con il SIO per esportare dati con lo scopo di:

- alimentare maschere di refertazione;
- richiamare altri applicativi (Insiel) con chiamate di contesto;
- aggiungere dati strumentali alla documentazione di referto;
- produrre un referto autonomamente e inviarlo al SIO per la conservazione;

dovrà ottemperare a quanto indicato nelle regole tecniche Fascicolo 2.0 e nella documentazione di HL7 Italia (http://www.hl7italia.it/hl7italia_D7/node/2359). Questo per rispettare nello specifico le modalità e le metodiche di creazione controllo e validazione dei referti, inclusa la tipologia di firma digitale applicata al documento.
Per le apparecchiature radiologiche è obbligatoria la possibilità di ottenere tramite report DICOM SR i dati di dose per la categorizzazione della procedura clinica in una delle classi di esposizione come

definito dalla Direttiva EURATOM 2013/59, recepita con d.lgs. 101/2020 e modificato dal d.lgs. 203/2022.

L'infrastruttura di ASFO ed integrazione

I sistemi oggetto di fornitura dovranno essere integrati ed interfacciati con l'infrastruttura informatica di rete e sistemistica di AsFO, secondo quanto riportato nel seguito.

I dispositivi dotati di connettività di rete (host) che necessitano di collegamento alla rete dati per svolgere le funzioni richieste, potranno essere inseriti nella LAN dell'azienda di destinazione seguendo uno degli scenari descritti nel seguito.

I firewall aziendali, utilizzati come ISFW a protezione di ciascuno dei contesti di rete descritti nel presente documento (reti e VLAN), sono tecnologicamente dei NGFW (Next Generation Firewall) dotati di funzionalità di statefull inspection e con application control attivo, conseguentemente tutti i sistemi e le applicazioni oggetto di fornitura, nonché i servizi di assistenza remota e manutenzione, anche erogati tramite VPN, dovranno essere compatibili con tali tecnologie. AsFO si riserva di bloccare qualunque tipologia di traffico ritenuto malevolo, in particolare a fronte di specifiche vulnerabilità che dovessero emergere nel corso della durata contrattuale.

Non sarà in generale consentita la fornitura di sistemi di cablaggio dati dedicati, a meno di casi particolari tecnicamente motivati, che dovranno essere esplicitati in offerta tecnica, motivati dettagliatamente ed approvati in ultima istanza da AsFO. Riguardo al cablaggio strutturato, dovranno essere utilizzati sempre e comunque i sistemi aziendali e gli eventuali ampliamenti necessari saranno eseguiti da AsFO. Dovranno essere indicati in offerta tecnica il numero e la dislocazione spaziale dei puti rete necessari al funzionamento dei sistemi oggetto di fornitura, indicando per ciascun punto l'eventuale necessità di installazione di dispositivi di separazione (Separation Device) conformi alle norme IEC 60601-1, la cui installazione sarà a carico di AsFO. Nel caso in cui l'aggiudicatario volesse comunque offrire servizi di posa in opera di cablaggio strutturato, dovrà sottostare alle indicazioni e validazioni progettuali di AsFO, oltre alle norme tecniche di riferimento.

AsFO potrà avvalersi di supporto specialistico per l'esecuzione di VA/PT (vulnerability assesment/penetration test) dei sistemi collegati alla propria rete. Pertanto il fornitore potrebbe essere chiamato da AsFO per fornire supporto ed eseguire verifiche funzionali legate all'esecuzione dei VA/PT in giornate programmate e concordate. Il costo per il ripristino del funzionamento è da intendersi completamente a carico del fornitore.

AsFO eseguirà, come parte del collaudo tecnico dell'apparecchiatura/sistema, una valutazione primaria volta ad una valutazione sulla sicurezza dei dispositivi i sistemi che verranno collegati alla rete aziendale di AsFO. A seguito di questo, verrà stilato un documento sottoscritto da ambo le parti dove si riportano le evidenze individuate durante l'attività di valutazione.

Scenari

Specifiche comuni

In funzione del tipo di sistema/soluzione/apparecchiatura verrà valutata la possibilità di applicare politiche di segmentazione della rete in coerenza con i fabbisogni aziendali, criticità e necessità per le apparecchiature. In quel caso i dispositivi oggetto di fornitura saranno integrati nella sole infrastrutture di rete di AsFO e saranno oggetto di policy di segmentazione e segregazione del traffico. La segmentazione del traffico verrà effettuata assegnando agli host stessi una specifica classe di indirizzi IP statici o tramite il servizio DHCP aziendale operando specifiche reservation in modo coerente con il piano di indirizzamenti di AsFO e verranno inseriti in una VLAN dedicata, assegnata

da AsFO stessa, dalla quale potranno effettuare solo l'eventuale traffico necessario per svolgere le funzioni richieste in capitolato e l'eventuale traffico relativo all'assistenza remota da parte del fornitore come definito nel documento DRW. La segregazione del traffico verrà garantita tramite configurazioni sui firewall aziendali (ISFW – Internal Segregation Firewall), stilate per rete IP e per porta, sulla base delle sole effettive necessità di traffico, evidenziate anche dal DRW per svolgere le funzioni richieste in capitolato. Il fornitore dovrà garantire piena collaborazione nella redazione di tali regole sui firewall aziendali (ISFW – Internal Segregation Firewall), per una durata complessiva di almeno un giorno lavorativo uomo e comunque fino al raggiungimento del risultato atteso. In ogni caso il traffico sarà consentito solo dalla periferia al centro e non da periferia a periferia, in particolare la rete IP/VLAN assegnata avrà visibilità di rete sulle reti IP/VLAN dei PC di AsFO solo in caso di necessità. AsFO si riserva di assegnare una o più reti IP/VLAN all'aggiudicatario in base alla specifica architettura proposta.

Nel caso in cui i dispositivi forniti siano di tipo trasportabile, palmari o mobile (tablet, smartphone, ecc) la connettività verrà garantita unicamente per mezzo di connessione cablata o Wi-Fi e solo per l'attività clinica, secondo quanto riportato precedentemente. Non sarà consentito in alcun caso il collegamento di tali dispositivi tramite le postazioni di lavoro (PC) – per esempio con collegamenti USB –. I collegamenti cablati dovranno essere realizzati con un adeguato grado di resistenza meccanica, nel caso per esempio dei dispositivi palmari o mobile, dovrà essere fornita una docking station.

Accessi VPN

Per le eventuali attività di assistenza remota, effettuate nel corso della durata del contratto dagli amministratori di sistema e o dai tecnici formalmente nominati dall'aggiudicatario, la connettività agli host oggetto di assistenza sarà garantita esclusivamente per mezzo dei sistemi VPN validati da AsFO. L'accesso verrà consentito solo a seguito di domanda sottoscritta digitalmente dal legale rappresentante o procuratore protempore dell'aggiudicatario – compilando il modulo standard allegato "Modulo B"– ed inviato via PEC alla casella PEC di AsFO, con allegati i documenti di identità e CF in corso di validità dei soggetti da abilitare. La connessione VPN dovrà essere di tipo client-to-site ed effettuata per mezzo di credenziali personali con bassi privilegi (livello user), ed in alcun caso saranno consentite connessioni di tipo site-to-site. A valle dell'instaurazione della connessione VPN, il collegamento ai singoli host oggetto di assistenza dovrà avvenire esclusivamente con gli strumenti scelti dall'aggiudicatario, sempre e comunque con modalità rispondenti al quadro legislativo e normativo vigente, solo a valle di validazione degli strumenti stessi da parte di AsFO. Il servizio di connessione remota VPN non verrà prestato all'aggiudicatario con livelli di servizio garantiti, perciò il servizio offerto dovrà essere organizzato in modo da sopperire all'indisponibilità del servizio VPN in altro modo (per esempio con intervento sul posto o altri sistemi di allarme e sicurezza), senza inficiare i livelli di servizio offerti né la sicurezza degli stessi, o evidenziando in offerta i livelli di servizio in caso di indisponibilità del servizio VPN.

Per quanto riguarda le eventuali attività di telemonitoraggio continuo da internet dei sistemi oggetto di assistenza gli scenari possibili sono due:

1. firewall di navigazione gestito dalla società in house della Regione Autonoma Friuli Venezia Giulia denominata Insiel SpA;
2. Firewall di navigazione gestito da AsFO;

In ogni caso i sistemi forniti potranno raggiungere solo un numero limitato di destinazioni internet, su specifiche porte; il traffico consentito sarà quello minimo necessario per il funzionamento dei sistemi e non sarà consentita la navigazione internet nonché l'esfiltrazione di dati tramite questo

canale. Verranno perciò effettuate specifiche abilitazioni basate su IP sorgente, IP destinazione e porta solo a seguito di domanda sottoscritta digitalmente dal legale rappresentante o procuratore protempore dell'aggiudicatario ed inviata via PEC alla casella PEC di AsFO o in risposta alla RdO/ODA effettuata, consegnando il "Modulo A" dettagliatamente compilato. L'aggiudicatario dovrà fornire la massima collaborazione in tal senso per la definizione delle suddette abilitazioni. Analogamente al servizio VPN individuato da AsFO, anche il servizio di connettività in uscita non verrà prestato all'aggiudicatario con livelli di servizio garantiti, perciò il servizio offerto dovrà essere organizzato in modo da sopperire all'indisponibilità del servizio in altro modo (per esempio con intervento sul posto o altri sistemi di allarme e sicurezza), senza inficiare i livelli di servizio offerti né la sicurezza degli stessi, o evidenziando in offerta i livelli di servizio in caso di indisponibilità del servizio.

CONTESTI

Di seguito si riportano i vari contesti a cui devono essere ricondotte tutte le soluzioni presentate in sede di offerta. Eventuali offerte non riconducibili a nessuna delle tre situazioni dovranno essere valutate di volta in volta e dovranno comunque rispettare le caratteristiche indicate nel documento con il più alto grado di attinenza al possibile contesto di affinità.

Contesto 1 Client o singolo DM/IVD

Singolo dispositivo o PC, collegabile alla rete aziendale, che riceve, invia o salva localmente informazioni di tipo diagnostico.

Contesto 2 Client Saas ibrido

Sistema client server, dove la parte server risiede all'interno dell'infrastruttura virtualizzata di proprietà di AsFO, la quale assicura alimentazione elettrica, raffrescamento e ripristino della macchina secondo le specifiche di backup concordate con il fornitore in fase di configurazione. Sarà cura dell'aggiudicatario tutto quanto il necessario al mantenimento della soluzione al top delle performance, e dovrà provvedere agli aggiornamenti lato applicativo e OS dandone preventiva comunicazione ad AsFO. Nel caso siano disponibili aggiornamenti dovrà essere cura dell'aggiudicatario avvisare tempestivamente AsFO per valutare e programmare le attività necessarie. Per l'esecuzione dei servizi verrà realizzato un utente di servizio con cui dovranno essere eseguiti i tasks propri dell'applicativo per garantirne il funzionamento. AsFO si riserva comunque la possibilità, a proprio insindacabile giudizio, di operare con la dismissione e spegnimento del sistema nel caso in cui si venisse rilevata una criticità che possa compromettere l'erogazione del servizio e di conseguenza possa generare un danno alla salute dei pazienti e operatori. In ogni momento AsFO potrà richiedere il passaggio al contesto 3 della soluzione durante tutto l'arco contrattuale senza alcun onere aggiuntivo.

RPO e RTO verranno stabiliti in base alla criticità del servizio.

Contesto 3 Client - Saas con edge

Vale tutto quanto come sopra, in aggiunta il sistema dovrà lavorare con replica sincrona nell'infrastruttura cloud messa a disposizione dall'aggiudicatario (di livello QC2 o QS2) e/o nello spazio Cloud messo a disposizione da AsFO (PSN oppure Cloud qualificato privato disponibile in convenzione e rispondente alla normativa vigente in relazione alla tipologia di servizio fornito). Sarà a carico dell'aggiudicatario verificare le performance della soluzione e che le stesse rispondano ai bisogni relativi all'erogazione del servizio.

La parte EDGE verrà gestita come da contesto 2, la parte in cloud dovrà essere fornita interamente in Saas. Il sito di erogazione primaria verrà definito sulla base della criticità del servizio e delle performance di connettività.

Requisiti ulteriori comuni ai contesti

Di seguito vengono definite le specifiche che i sistemi forniti dovranno rispettare, sia nel caso di non collegamento in rete, sia di realizzazione aderente ai vari contesti, relativamente ad aspetti generali della sfera dell'IT (Information Technology) con particolare riferimento alla sicurezza informatica (security).

Vale in ogni caso il principio generale per cui la sicurezza informatica è un fattore intrinseco dell'architettura dei sistemi oggetto della presente fornitura e delle caratteristiche tecniche degli elementi che li compongono; perciò l'aggiudicatario dovrà garantire che, sia l'architettura che gli elementi, siano progettati, implementati e manutenuti nel tempo in modo da minimizzare il rischio informatico residuo (sia di "attacchi ai sistemi" che di "attacchi dai sistemi") e comunque in osservanza delle normative e best practice già citate dal primo paragrafo del presente documento e sempre in coerenza con il paradigma "Zero Trust".

Potrebbero eseguite periodicamente da AsFO o da personale a tal scopo incaricato procedure di Vulnerability Assessment e Penetration Test e l'aggiudicatario si impegna pertanto a risolvere criticità o vulnerabilità che dovessero in tal modo emergere. Analogamente l'aggiudicatario si impegna a collaborare con il SOC (Security Operation Center) di AsFO per il miglioramento continuo dei sistemi forniti.

Inoltre i sistemi forniti dovranno rispettare le seguenti prescrizioni.

In generale, tutti gli elementi forniti non dovranno essere in alcun caso fuori supporto tecnico del fabbricante o a fine ciclo di vita (end-of-life) e comunque non dovranno trovarsi in tale stato per tutta la durata contrattuale.

In generale, tutti i software forniti dovranno essere:

- coerenti con la necessità di richiedere applicazioni, servizi e procedure privacy by design e privacy by default per ogni percorso di trattamento. Tutti i sistemi devono essere costruiti per proteggere i dati trattati e farlo come impostazione predefinita. L'aggiudicatario è tenuto a fornire documentazione delle misure implementate anche allo scopo di permettere le necessarie valutazioni al Titolare;
- intuitivi e di facile utilizzo, ad ogni livello di accesso ed in ogni configurazione, per tutti gli operatori (a prescindere dal ruolo);
- dotati di impostazioni internazionali di Microsoft Windows (se presente) IT standard, comprese le tastiere, allo scopo di non incorrere in nessun caso in errori nelle date, nei dati numerici e nei dati personali locali;
- stabili, in particolare che siano in grado di gestire le eccezioni;
- sicuri, sia dal punto di vista della sicurezza informatica che della qualità delle funzioni svolte;
- ottimizzati, in termini di rapporto tra uso delle risorse e prestazioni;
- sviluppati tenendo conto dei principi del "ciclo di vita del software" e dell'"analisi del rischio", secondo le norme tecniche (o principi e metodologie almeno equivalenti) e le best practice internazionali; in ogni caso non dovranno utilizzare librerie deprecate e/o obsolete, né dovranno essere scritti e sviluppati con versioni del linguaggio di programmazione fuori supporto tecnico del fabbricante o a fine ciclo di vita (end-of-life) e comunque non dovranno trovarsi in tale stato per tutta la durata contrattuale;

- pensati, progettati e realizzati nel rispetto del quadro legislativo vigente, nonché in modo da non mettere in alcun caso gli operatori in condizione di violare il quadro legislativo stesso nell'espletamento del normale utilizzo dei sistemi;
- installati e configurati per essere utilizzati, in condizioni di massima sicurezza e funzionalità, così come descritto nel presente documento;
- manutenuti e gestiti in modo da conservare e mantenere stabili nel tempo tutte le caratteristiche possedute al momento del collaudo definitivo.

In particolare, tutti i software forniti che verranno installati su dispositivi collegati alle LAN aziendali e inseriti nei rispettivi domini dovranno essere eseguiti sempre:

- in un contesto user space per i client,
- come servizio per tutti i server,
- come servizio per i client se non è richiesta interazione con l'operatore,

ed in ogni caso non dovranno essere modificati in alcun modo i permessi di default del file system e del registro di sistema Microsoft (ove presente).

In particolare, per quanto concerne le configurazioni:

- quelle degli applicativi server dovranno risiedere in database e comunque mai sui dischi locali dei PC client;
- quelle globali degli applicativi client (ovvero non riferite alle personalizzazioni dei singoli account) dovranno risiedere in un file nella cartella di installazione dell'applicativo (a cui quindi avranno accesso solo gli utenti con ruolo Amministratore) oppure nella cartelle %HOMEDRIVE%\ProgramData, oppure nel registro di sistema (ove presente) nella sottochiave appositamente creata in fase di installazione in HKEY_LOCAL_MACHINE\SOFTWARE, ed in ogni caso informazioni critiche in termini di sicurezza e funzionalità (a titolo di esempio non esaustivo: le stringhe di connessione ai database, le credenziali necessarie per instaurare eventuali altre connessioni client/server, ecc.) dovranno essere cifrate almeno con algoritmo AES256;
- quelle personali degli applicativi client (ovvero riferite alle personalizzazioni dei singoli account) dovranno risiedere nel profilo dell'account a cui si riferiscono (ove presente).

Ovvero, in ogni caso non dovranno risiedere configurazioni globali degli applicativi client nei profili degli account, né altresì configurazioni personali degli applicativi client fuori dai profili degli account.

In particolare, a titolo esemplificativo e non esaustivo, si ricorda che, anche nel perimetro delle prescrizioni previste dalla Circolare AGID 18 aprile 2017, n. 2/2017, recante "Misure minime di sicurezza ICT per le pubbliche amministrazioni", i sistemi forniti:

- non devono prevedere nessun account locale;
- non devono prevedere nessun account impersonale per gli operatori e account di servizio solo se del tipo gMSA, group Managed Service Account;
- devono consentire azioni di software inventory;
- devono poter essere distribuiti in "package" fruibili dal sistema di distribuzione software;
- devono utilizzare solo sistemi di comunicazione sicuri (crittati);
- devono rispettare le tecnologie di protezione delle banche dati di dati personali e sensibili;

- devono consentire le valutazioni di vulnerabilità e il fornitore deve adoperarsi per la risoluzione in tempi certi ed accettabili delle anomalie rilevate da AsFO o dalle aziende da AsFO deputate.

In ogni caso i software oggetto di fornitura non dovranno fare uso di Applet Java e ActiveX.

Come indicato in premessa, l'aggiudicatario verrà designato responsabile ex art.28 del GDPR, ed in quest'ambito dovrà, tra l'altro, inviare, nel rispetto delle procedure di AsFO, le richieste di abilitazione degli incaricati e degli amministratori afferenti all'aggiudicatario (anche quelle necessarie per lo svolgimento delle attività di assistenza remota). I relativi account e le relative autorizzazioni verranno sempre erogate a livello personale, secondo le varie procedure aziendali ed in ogni caso con i privilegi necessari e sufficienti allo svolgimento delle mansioni di competenza.

Per quanto concerne gli "account amministrativi" (ovvero ogni account a cui è associato un ruolo Amministratore o che è dotato di privilegi amministrativi o che consenta di svolgere funzioni di amministratore su qualunque macchina, sistema o applicativo fornito), questi:

- potranno, nel caso di account amministrativi locali di default (a titolo di esempio non esaustivo: "admin", "administrator", "root", ecc.), essere impersonali e dovranno essere tutti comunicati ad AsFO ove richiesto, AsFO potrà modificarne le password e che li conserverà secondo le proprie procedure standard di sicurezza; in ogni caso non dovranno essere configurati account amministrativi locali ulteriori rispetto a quelli di default; ove non richiesto da AsFO la gestione e responsabilità si intende completamente a carico dell'aggiudicatario;
- dovranno, nel caso di account amministrativi non locali che consentano l'accesso interattivo a macchine/sistemi/applicativi collegati alla LAN di AsFO, essere sempre personali e rispettare quanto riportato nel presente documento relativamente alle modalità di autenticazione (authentication) degli operatori per mezzo di account – e relative credenziali – personali;
- non dovranno, nel caso di account amministrativi impersonali, essere in alcun caso presenti, se non del tipo gMSA;
- dovranno, nel caso di tutti gli account di sistemi non in LAN, essere gestiti a cura e responsabilità dell'aggiudicatario;
- potranno, nel caso di account amministrativi di macchine/sistemi/applicativi non collegati alla LAN di AsFO, essere impersonali e dovranno essere tutti comunicati ove richiesto, AsFO potrà modificarne le password e che li conserverà secondo le proprie procedure standard di sicurezza; in ogni caso non dovranno essere configurati account amministrativi in numero maggiore dello stretto necessario; ove non richiesti la gestione e responsabilità si intende a carico dell'aggiudicatario;

  in tal caso, ovvero per quanto concerne gli account impersonali, consentiti solo secondo quanto riportato nel punto precedente, questi non dovranno in alcun caso permettere:
  - di modificare le configurazioni, impostazioni e settaggi di macchine/sistemi/applicativi;
  - di visualizzare, modificare o cancellare dati personali diversi da quelli eventualmente trattati contestualmente all'uso dell'account stesso.

Eventuali dati personali salvati in ulteriori archivi, diversi da quelli descritti nel presente documento, saranno ammessi solo con funzioni di "archivi provvisori", ovvero di passaggio intermedio dei dati prima dell'invio agli archivi definitivi. I dati personali devono permanere negli archivi provvisori il minor tempo possibile, ovvero per un tempo massimo che sia configurabile e che

in ogni caso non superi le 24 ore naturali, con l'implementazione di opportune procedure di cancellazione automatica che non consentano il recupero locale dei dati.

Ogni attività di aggiornamento, dovrà essere prima comunicata e validata da AsFO, testata e rilasciata nelle modalità concordate anche in coerenza con il possibile impatto sulla capacità di erogazione delle prestazioni sanitarie di AsFO. Tutte le attività di aggiornamento dovranno necessariamente essere indicate nel "Modulo C DAPS" che rappresenta parte integrante della documentazione relativa alla fornitura e potrà essere utilizzata per il rilascio della regolare esecuzione del servizio/fornitura affidato/a.

In ogni caso l'accesso agli archivi di dati personali (anche provvisori) dovrà avvenire solo da parte degli account personali e degli account gMSA autorizzati, sulla base di opportuni permessi settati in modo che il livello dei privilegi di accesso sia il più basso possibile e che l'accesso ai dati avvenga sempre per tramite dell'applicativo e non direttamente da parte dell'account.

Non è consentita l'archiviazione, anche temporanea ed anche in forma anonima, dei dati su macchine situate esternamente rispetto alla rete di AsFO, salvo esplicita autorizzazione.

Non sarà in alcun caso consentita la fornitura ed installazione di apparati attivi di rete standard (switch, router, firewall, access point Wi-Fi, VPN concentrator, Mi-Fi etc.) a meno di eccezioni concordate e validate a seguito di presentazione di adeguata documentazione tecnica che ne giustifichi la necessità. In particolare: nel caso di apparati di sicurezza, l'aggiudicatario si impegna, come precedentemente riportato, a trasferire le logiche di sicurezza sui firewall Aziendali (ISFW – Internal Segregation Firewall); nel caso di apparati per la connettività remota, l'aggiudicatario si impegna a far uso degli strumenti aziendali messi a disposizione da AsFO, come precedentemente riportato.

PACS

Il sistema PACS di AsFO è Suitestensa di Esaote S.p.A., configurato su livelli, che confluiscono nel PACS centrale di ASFO (P.O. di Pordenone) e per la parte di conservazione legale in Regione.
La connettività tra i vari livelli del PACS è garantita all'interno della rete Regionale FVG RUPAR, gestita da Insiel S.p.A.
Il Sistema RIS attualmente in uso, che fornisce anche il servizio di modality worklist è G2 Clinico, di Insiel S.p.A. Il servizio RIS è erogato all'interno della rete Regionale FVG RUPAR, gestita da Insiel S.p.A.
Le apparecchiature dovranno essere fornite complete delle licenze per la messa in rete e rispettare il seguente standard: DICOM 3.0 completo delle classi worklist, store, print, q/r, mpps, sc.
Per i dispositivi offerti dovrà essere data evidenza della corrispondenza ai profili di integrazione IHE.
Tutte le licenze d'uso del software non devono avere scadenza o limiti temporali che possano determinare blocchi funzionali e/o che richiedano oneri per ASFO.
Per ogni apparecchiatura messa a disposizione dall'OE dovranno essere forniti:

- copia dell'"INTEGRATION STATEMENTS IHE" o in subordine, copia del Conformance Statement Standard DICOM 3.

LIS

Specifiche di integrazione con il LIS
I sistemi oggetto di fornitura dovranno essere marcati CE ai sensi del Regolamento IVDR relativa ai dispositivi medico diagnostici in vitro recepita con d.Lgs. 138/2022, ove applicabile.
Tutti i software di interpretazione dei dati oggetto di fornitura dovranno colloquiare bidirezionalmente con il LIS (Laboratory Information System) Aziendale. Il LIS attualmente in uso (non oggetto di fornitura) è DNLab di NoemaLife S.p.A. fornito da Insiel S.p.a., gestito e manutenuto da

Insiel S.p.a. in tutta la Regione Friuli Venezia Giulia. Attualmente, è previsto che il DNLab si interfacci con la strumentazione analitica per mezzo del middleware HALIA di NoemaLife gestito da Insiel S.p.A. Pertanto, l'aggiudicatario dovrà interfacciare i software di interpretazione forniti con il sistema in uso al momento della consegna e, qualora questo sia DNA, si intende compreso nel prezzo di fornitura la successiva migrazione (secondo i tempi che saranno indicati) ad HALIA.

L'interfacciamento tra strumento/WAM (Work Area Manager)/Middleware e Halia dovrà avvenire tramite socket TCP e solo in caso di vincolo tecnico potrà essere realizzato tramite interfacciamento seriale. Tali casistiche andranno giustificate e motivato tecnicamente in offerta ed in ogni caso tali soluzioni dovranno essere insindacabilmente validate da AsFO; in tal caso dovranno essere oggetto di fornitura i convertitori seriale/ethernet che si intendono perciò garantiti e certificati dal fabbricante per la specifica destinazione d'uso.

Versione	**Data**
0.4	**14/1/2025**

Documenti eventuali da allegare

Modulo A

Documento Riepilogativo Workflow "DRW"

Nel caso di sistemi complessi, non dispositivi stand alone (anche stand alone ma che dovranno essere integrati con l'infrastruttura LAN di AsFO) si richiede di completare quanto previsto per contestualizzare le specifiche di funzionamento ed integrazione con AsFO.

Si richiede di fornire in offerta tecnica un "documento riepilogativo workflow" (esempio DRW Documento A), firmato digitalmente dove dev'essere evidenziato quanto segue:

- tipologia di architettura (anche a livello grafico);
- tipologie di trasmissioni indicando eventualmente il protocollo, la porta e la tipologia di dati trasmessi;
- elementi coinvolti (server, client, applicativo) e responsabilità di gestione, indicando eventualmente fornitori terzi e tipologia di accordo contrattuale tra fornitore e partner.

Prima parte grafica.

Seconda parte descrittiva: indicare attori coinvolti, tipologia di comunicazione (protocollo, porte, …), figura responsabile

Modulo B

Modulo richiesta VPN

Modulo C

Documento Aggiornamenti e Patch Sicurezza "DAPS"

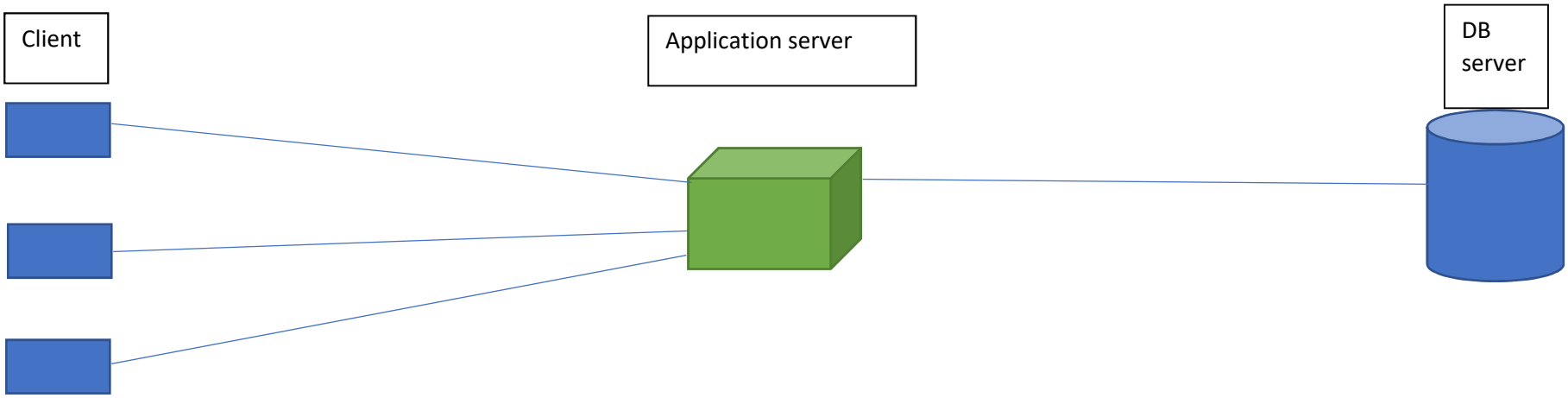
Documento che verrà mantenuto aggiornato dall'OE per tutta la durata del contratto e reso disponibile ad AsFO in qualsiasi momento per verificare lo stato di messa in produzione di aggiornamenti di sicurezza/nuove funzionalità/test.

AS FO Azienda sanitaria Friuli Occidentale REGIONE AUTONOMA FRIULI VENEZIA GIULIA	**Azienda sanitaria Friuli Occidentale** **Modulo A** **Documento Riepilogativo Workflow "DRW"**

Documento Riepilogativo Workflow "DRW"

Parte grafica

esempio non esaustivo



Seconda parte descrittiva (esempio)

Elemento	descrizione	Ubicazione	Destinatario trasmissione	Tipologia di comunicazione	Responsabile/gestore	Note
1	Software installato su PC fornito da ASFO/OE	In Azienda sanitaria	Application server	https porta 443	OE	Requisiti minimi: versione windows, versione .NET
2	Application server	In cloud oggetto di fornitura	DB server	TCP porta 1433	OE	
3	…	…	…	…	…	…

AS FO Azienda sanitaria Friuli Occidentale REGIONE AUTONOMA FRIULI VENEZIA GIULIA	**Azienda sanitaria Friuli Occidentale** **Modulo B** **Modulo richiesta VPN**

Modulo richiesta VPN

Il presente documento fa riferimento alla richiesta di collegamento tra una sede da Voi definita e AsFO per l'esecuzione di attività di:
- configurazione;
- manutenzione;

da eseguire da remoto su apparati localizzati all'interno della LAN di AsFO.
La S.C. Gestione e Innovazione Tecnologie, richiede alla Vostra Ditta di inviare il presente modulo completo in ogni sua parte al seguente indirizzo mail: **asfo.protgen@certsanita.fvg.it**

Dati richiedente

Il sottoscritto, ……

nato a ……., il……..

in nome dell'Azienda ……..

con sede legale ……..

in qualità di ……..

RICHIEDO

una coppia di credenziali personali per poter instaurare una connessione tramite VPN con AsFO per l'esecuzione di attività di:

- configurazione;
- manutenzione;

da eseguire da remoto su apparati localizzati all'interno della infrastruttura di AsFO per il seguente personale dipendente dell'azienda sopra indicata:

Nome	Cognome	CF	Qualifica	Numero di cellulare	Mail aziendale

Dichiaro inoltre, relativamente a obblighi di riservatezza, segretezza e sicurezza nei collegamenti da remoto

di accettare quanto segue:

1. mantenere la più assoluta riservatezza e segretezza sulle informazioni acquisite durante lo svolgimento dell'attività. Per informazioni si intendono sia le informazioni necessarie per aprire/chiudere il collegamento remoto, sia i dati che vengono trattati durante la sessione di collegamento remoto. Accedere ai dati strettamente necessari all'espletamento dell'attività di cui è stata richiesta l'esecuzione. Ovvero a espletare l'attività nel pieno rispetto del D.lgs. 196/2003 ("Testo Unico della Privacy - Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali") e del Regolamento Europeo 679/2016 "GDPR" sulla protezione dei dati personali recepito con D.lgs. 101/2018 e successive modificazioni e integrazioni;

2. non divulgare in nessun modo le informazioni di cui al punto 1;

3. utilizzare il collegamento per i soli scopi ed alle condizioni definiti dal contratto di assistenza e dalla scheda di collegamento remoto e modalità di connessione relativa al collegamento (che sarà redatta congiuntamente durante l'attivazione del collegamento);

4. salvo il caso di collegamenti tramite VPN o altre soluzioni concordate con S.C. Gestione Innovazione Tecnologie, **non** utilizzare applicativi che facciano uso di protocolli di comunicazione SSL (https, ssh, ecc.) ed in generale meccanismi di crittografia che impediscano l'interpretazione dei pacchetti in transito da parte di personale incaricato AsFO;

5. nominare il proprio responsabile dei trattamenti effettuati con il collegamento remoto;

6. inviare un elenco del personale che utilizzerà la connessione messa a disposizione, precisando se dipendente interno o consulente;

7. garantire che i propri incaricati - che effettuano trattamenti con il collegamento remoto - operino nel pieno rispetto dei punti 1, 2 e 3.

INOLTRE PRENDO ATTO CHE:

1. tutto il traffico prodotto tramite il collegamento remoto può essere monitorato, i pacchetti di dati vengono salvati in file di log e mantenuti per tutto il tempo che la S.C. Gestione e Innovazione Tecnologie riterrà opportuno, e potrebbero in qualsiasi momento essere utilizzati per scopi statistici o di verifica delle operazioni effettuate;

2. AsFO potrà decidere in qualsiasi momento di disabilitare temporaneamente o definitivamente l'accesso, qualora ne ravvisi necessità per qualsiasi ragione.

Il/La sottoscritto/a dichiara, ai sensi Regolamento UE 2016/679, di autorizzare il trattamento dei propri dati personali contenuti nel presente modulo, anche con strumenti informatici, esclusivamente nell'ambito del procedimento per il quale la presente dichiarazione viene resa.

Data

……./……/…………

COGNOME e NOME   FIRMA

______________________________   ____________________

AS FO Azienda sanitaria Friuli Occidentale REGIONE AUTONOMA FRIULI VENEZIA GIULIA	**Azienda sanitaria Friuli Occidentale** **Modulo C** **Documento Aggiornamenti e Patch Sicurezza "DAPS"**

Documento Aggiornamenti e Patch Sicurezza "DAPS"

Data messa in produzione	Descrizione rilascio/aggiornamento	Reparto coinvolto	Date prove pre produzione (inizio e fine)	Reparto coinvolto	Referente per l'aggiornamento

MD security

Question ID	Question		See note	IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
DOC-1	Manufacturer Name Supplier Name					
DOC-2	Device/System Description					
DOC-3	Device Model(s)					
DOC-4	Document ID					
DOC-5	Manufacturer Contact Supplier Contact					
DOC-6	Type of connection to corporate network and purpose Need for internet connection and purpose					
DOC-7	Document Release Date					
DOC-8	Does the manufacturer have a vulnerability assessment program for this device(s) or system?					
DOC-9	ISAO: Is the manufacturer part of an Information Sharing and Analysis Organization?					
DOC-10	Diagram: Is a network or data flow diagram available that indicates connections to other system components or expected external resources?					
DOC-11	SaMD: Is the device Software as a Medical Device (i.e. software-only, no hardware)?					
DOC-11.1	Does the SaMD contain an operating system?					
DOC-11.2	Does the SaMD rely on an owner/operator provided operating system?					
DOC-11.3	Is the SaMD hosted by the manufacturer?					
DOC-11.4	Is the SaMD hosted by the customer?					
		Yes, No, N/A, or See Note	Note #			
	MANAGEMENT OF PERSONALLY IDENTIFIABLE INFORMATION			IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
MPII-1	Can this device display, transmit, store, or modify personally identifiable information (e.g. electronic Protected Health Information (ePHI))?				AR-2	A.15.1.4
MPII-2	Does the device maintain personally identifiable information?				AR-2	A.15.1.4
MPII-2.1	Does the device maintain personally identifiable information temporarily in volatile memory (i.e., until cleared by power-off or reset)?				AR-2	A.15.1.4
MPII-2.2	Does the device store personally identifiable information persistently on internal media?					
MPII-2.3	Is personally identifiable information preserved in the device's non-volatile memory until explicitly erased?					
MPII-2.4	Does the device store personally identifiable information in a database?					
MPII-2.5	Does the device allow configuration to automatically delete local personally identifiable information after it is stored to a long term solution?				AR-2	A.15.1.4

MPII-2.6	Does the device import/export personally identifiable information with other systems (e.g., a wearable monitoring device might export personally identifiable information to a server)?	_____	__	AR-2	A.15.1.4
MPII-2.7	Does the device maintain personally identifiable information when powered off, or during power service interruptions?	_____	__	AR-2	A.15.1.4
MPII-2.8	Does the device allow the internal media to be removed by a service technician (e.g., for separate destruction or customer retention)?	_____	__		
MPII-2.9	Does the device allow personally identifiable information records be stored in a separate location from the device's operating system (i.e. secondary internal drive, alternate drive partition, or remote storage location)?	_____		AR-2	A.15.1.4
MPII-3	Does the device have mechanisms used for the transmitting, importing/exporting of personally identifiable information?	_____	__	AR-2	A.15.1.4
MPII-3.1	Does the device display personally identifiable information (e.g., video display, etc.)?	_____	__	AR-2	A.15.1.4
MPII-3.2	Does the device generate hardcopy reports or images containing personally identifiable information?	_____	__	AR-2	A.15.1.4
MPII-3.3	Does the device retrieve personally identifiable information from or record personally identifiable information to removable media (e.g., removable-HDD, USB memory, DVD-R/RW,CD-R/RW, tape, CF/SD card, memory stick, etc.)?	_____	__	AR-2	A.15.1.4
MPII-3.4	Does the device transmit/receive or import/export personally identifiable information via dedicated cable connection (e.g., RS-232, RS-423, USB, FireWire, etc.)?	_____	__	AR-2	A.15.1.4
MPII-3.5	Does the device transmit/receive personally identifiable information via a wired network connection (e.g., RJ45, fiber optic, etc.)?	_____	__	AR-2	A.15.1.4
MPII-3.6	Does the device transmit/receive personally identifiable information via a wireless network connection (e.g., WiFi, Bluetooth, NFC, infrared, cellular, etc.)?	_____	__	AR-2	A.15.1.4
MPII-3.7	Does the device transmit/receive personally identifiable information over an external network (e.g., Internet)?	_____	__	AR-2	A.15.1.4
MPII-3.8	Does the device import personally identifiable information via scanning a document?	_____			
MPII-3.9	Does the device transmit/receive personally identifiable information via a proprietary protocol?	_____			
MPII-3.10	Does the device use any other mechanism to transmit, import or export personally identifiable information?	_____	__	AR-2	A.15.1.4
Management of Private Data notes:				AR-2	A.15.1.4

	AUTOMATIC LOGOFF (ALOF)			IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
	The device's ability to prevent access and misuse by unauthorized users if device is left idle for a period of time.					
ALOF-1	Can the device be configured to force reauthorization of logged-in user(s) after a predetermined length of inactivity (e.g., auto-logoff, session lock, password protected screen saver)?	_____	—	Section 5.1, ALOF	AC-12	None
ALOF-2	Is the length of inactivity time before auto-logoff/screen lock user or administrator configurable?	_____	—	Section 5.1, ALOF	AC-11	A.11.2.8, A.11.2.9

	AUDIT CONTROLS (AUDT)			IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
	The ability to reliably audit activity on the device.					
AUDT-1	Can the medical device create additional audit logs or reports beyond standard operating system logs?	_____	—	Section 5.2, AUDT	AU-1	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
AUDT-1.1	Does the audit log record a USER ID?	_____	—			
AUDT-1.2	Does other personally identifiable information exist in the audit trail?			Section 5.2, AUDT	AU-2	None
AUDT-2	Are events recorded in an audit log? If yes, indicate which of the following events are recorded in the audit log:	_____	—	Section 5.2, AUDT	AU-2	None
AUDT-2.1	Successful login/logout attempts?	_____	—	Section 5.2, AUDT	AU-2	None
AUDT-2.2	Unsuccessful login/logout attempts?	_____	—	Section 5.2, AUDT	AU-2	None
AUDT-2.3	Modification of user privileges?	_____	—	Section 5.2, AUDT	AU-2	None
AUDT-2.4	Creation/modification/deletion of users?	_____	—	Section 5.2, AUDT	AU-2	None
AUDT-2.5	Presentation of clinical or PII data (e.g. display, print)?	_____	—	Section 5.2, AUDT	AU-2	None
AUDT-2.6	Creation/modification/deletion of data?	_____	—	Section 5.2, AUDT	AU-2	None
AUDT-2.7	Import/export of data from removable media (e.g. USB drive, external hard drive, DVD)?	_____	—	Section 5.2, AUDT	AU-2	None
AUDT-2.8	Receipt/transmission of data or commands over a network or point-to-point connection?	_____	—	Section 5.2, AUDT	AU-2	None
AUDT-2.8.1	Remote or on-site support?	_____	—	Section 5.2, AUDT	AU-2	None
AUDT-2.8.2	Application Programming Interface (API) and similar activity?	_____	—	Section 5.2, AUDT	AU-2	None
AUDT-2.9	Emergency access?	_____	—	Section 5.2, AUDT	AU-2	None
AUDT-2.10	Other events (e.g., software updates)?	_____	—	Section 5.2, AUDT	AU-2	None
AUDT-2.11	Is the audit capability documented in more detail?	_____	—	Section 5.2, AUDT	AU-2	None
AUDT-3	Can the owner/operator define or select which events are recorded in the audit log?			Section 5.2, AUDT	AU-2	None
AUDT-4	Is a list of data attributes that are captured in the audit log for an event available?	_____	—	Section 5.2, AUDT	AU-2	None

AUDT-4.1	Does the audit log record date/time?	_____	—	Section 5.2, AUDT	AU-2	None
AUDT-4.1.1	Can date and time be synchronized by Network Time Protocol (NTP) or equivalent time source?	_____	—	Section 5.2, AUDT	AU-2	None
AUDT-5	Can audit log content be exported?	_____	—	Section 5.2, AUDT	AU-2	None
AUDT-5.1	Via physical media?	_____	—			
AUDT-5.2	Via IHE Audit Trail and Node Authentication (ATNA) profile to SIEM?	_____	—			
AUDT-5.3	Via Other communications (e.g., external service device, mobile applications)?	_____	—			
AUDT-5.4	Are audit logs encrypted in transit or on storage media?	_____	—			
AUDT-6	Can audit logs be monitored/reviewed by owner/operator?	_____	—			
AUDT-7	Are audit logs protected from modification?	_____	—	Section 5.2, AUDT	AU-2	None
AUDT-7.1	Are audit logs protected from access?					
AUDT-8	Can audit logs be analyzed by the device?	_____	—	Section 5.2, AUDT	AU-2	None
	AUTHORIZATION (AUTH)			IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
	The ability of the device to determine the authorization of users.					
AUTH-1	Does the device prevent access to unauthorized users through user login requirements or other mechanism?	_____	—	Section 5.3, AUTH	IA-2	A.9.2.1
AUTH-1.1	Can the device be configured to use federated credentials management of users for authorization (e.g., LDAP, OAuth)?	_____	—	Section 5.3, AUTH	IA-2	A.9.2.1
AUTH-1.2	Can the customer push group policies to the device (e.g., Active Directory)?	_____	—	Section 5.3, AUTH	IA-2	A.9.2.1
AUTH-1.3	Are any special groups, organizational units, or group policies required?	_____	—	Section 5.3, AUTH	IA-2	A.9.2.1
AUTH-2	Can users be assigned different privilege levels based on 'role' (e.g., user, administrator, and/or service, etc.)?	_____	—	Section 5.3, AUTH	IA-2	A.9.2.1
AUTH-3	Can the device owner/operator grant themselves unrestricted administrative privileges (e.g., access operating system or application via local root or administrator account)?	_____	—	Section 5.3, AUTH	IA-2	A.9.2.1
AUTH-4	Does the device authorize or control all API access requests?	_____	—	Section 5.3, AUTH	IA-2	A.9.2.1
AUTH-5	Does the device run in a restricted access mode, or 'kiosk mode', by default?	_____	—			
	CYBER SECURITY PRODUCT UPGRADES (CSUP)			IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
	The ability of on-site service staff, remote service staff, or authorized customer staff to install/upgrade device's security patches.					

CSUP-1	Does the device contain any software or firmware which may require security updates during its operational life, either from the device manufacturer or from a third-party manufacturer of the software/firmware? If no, answer "N/A" to questions in this section.	_____	__
CSUP-2	Does the device contain an Operating System? If yes, complete 2.1-2.4.	_____	__
CSUP-2.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	_____	__
CSUP-2.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	_____	__
CSUP-2.3	Does the device have the capability to receive remote installation of patches or software updates?	_____	__
CSUP-2.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	_____	__
CSUP-3	Does the device contain Drivers and Firmware? If yes, complete 3.1-3.4.	_____	__
CSUP-3.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	_____	__
CSUP-3.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	_____	__
CSUP-3.3	Does the device have the capability to receive remote installation of patches or software updates?	_____	__
CSUP-3.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	_____	__
CSUP-4	Does the device contain Anti-Malware Software? If yes, complete 4.1-4.4.	_____	__
CSUP-4.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	_____	__
CSUP-4.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	_____	__
CSUP-4.3	Does the device have the capability to receive remote installation of patches or software updates?	_____	__
CSUP-4.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	_____	__
CSUP-5	Does the device contain Non-Operating System commercial off-the-shelf components? If yes, complete 5.1-5.4.	_____	__

CSUP-5.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	_____	__			
CSUP-5.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	_____	__			
CSUP-5.3	Does the device have the capability to receive remote installation of patches or software updates?	_____	__			
CSUP-5.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	_____	__			
CSUP-6	Does the device contain other software components (e.g., asset management software, license management)? If yes, please provide details or refernce in notes and complete 6.1-6.4.	_____	__			
CSUP-6.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	_____	__			
CSUP-6.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	_____	__			
CSUP-6.3	Does the device have the capability to receive remote installation of patches or software updates?	_____	__			
CSUP-6.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	_____	__			
CSUP-7	Does the manufacturer notify the customer when updates are approved for installation?	_____	__			
CSUP-8	Does the device perform automatic installation of software updates?	_____	__			
CSUP-9	Does the manufacturer have an approved list of third-party software that can be installed on the device?	_____	__			
CSUP-10	Can the owner/operator install manufacturer-approved third-party software on the device themselves?	_____	__			
CSUP-10.1	Does the system have mechanism in place to prevent installation of unapproved software?	_____	__			
CSUP-11	Does the manufacturer have a process in place to assess device vulnerabilities and updates?	_____	__			
CSUP-11.1	Does the manufacturer provide customers with review and approval status of updates?	_____	__			
CSUP-11.2	Is there an update review cycle for the device?	_____	__			

		IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
HEALTH DATA DE-IDENTIFICATION (DIDT)				
The ability of the device to directly remove information that allows identification of a person.				

DIDT-1	Does the device provide an integral capability to de-identify personally identifiable information?	_____	—	Section 5.6, DIDT	None	ISO 27038
DIDT-1.1	Does the device support de-identification profiles that comply with the DICOM standard for de-identification?	_____	—	Section 5.6, DIDT	None	ISO 27038
	DATA BACKUP AND DISASTER RECOVERY (DTBK)			IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
	The ability to recover after damage or destruction of device data, hardware, software, or site configuration information.					
DTBK-1	Does the device maintain long term primary storage of personally identifiable information / patient information (e.g. PACS)?	_____	—			
DTBK-2	Does the device have a “factory reset” function to restore the original device settings as provided by the manufacturer?	_____	—	Section 5.7, DTBK	CP-9	A.12.3.1
DTBK-3	Does the device have an integral data backup capability to removable media?	_____	—	Section 5.7, DTBK	CP-9	A.12.3.1
DTBK-4	Does the device have an integral data backup capability to remote storage?					
DTBK-5	Does the device have a backup capability for system configuration information, patch restoration, and software restoration?					
DTBK-6	Does the device provide the capability to check the integrity and authenticity of a backup?	_____	—	Section 5.7, DTBK	CP-9	A.12.3.1
	EMERGENCY ACCESS (EMRG)			IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
	The ability of the device user to access personally identifiable information in case of a medical emergency situation that requires immediate access to stored personally identifiable information.					
EMRG-1	Does the device incorporate an emergency access (i.e. “break-glass”) feature?	_____	—	Section 5.8, EMRG	SI-17	None
	HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU)			IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
	How the device ensures that the stored data on the device has not been altered or destroyed in a non-authorized manner and is from the originator.					
IGAU-1	Does the device provide data integrity checking mechanisms of stored health data (e.g., hash or digital signature)?	_____	—	Section 5.9, IGAU	SC-28	A.18.1.3
IGAU-2	Does the device provide error/failure protection and recovery mechanisms for stored health data (e.g., RAID-5)?	_____	—	Section 5.9, IGAU	SC-28	A.18.1.3
	MALWARE DETECTION/PROTECTION (MLDP)			IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
	The ability of the device to effectively prevent, detect and remove malicious software (malware).					

MLDP-1	Is the device capable of hosting executable software?	_____	__	Section 5.10, MLDP		
MLDP-2	Does the device support the use of anti-malware software (or other anti-malware mechanism)? Provide details or reference in notes.	_____	__	Section 5.10, MLDP	SI-3	A.12.2.1
MLDP-2.1	Does the device include anti-malware software by default?	_____	__	Section 5.10, MLDP	CM-5	A.9.2.3, A.9.4.5, A.12.1.2, A.12.1.4, A.12.5.1
MLDP-2.2	Does the device have anti-malware software available as an option?	_____	__	Section 5.10, MLDP	AU-6	A.12.4.1, A.16.1.2, A.16.1.4
MLDP-2.3	Does the device documentation allow the owner/operator to install or update anti-malware software?	_____	__	Section 5.10, MLDP	CP-10	A.17.1.2
MLDP-2.4	Can the device owner/operator independently (re-)configure anti-malware settings?	_____	__	Section 5.10, MLDP	AU-2	None
MLDP-2.5	Does notification of malware detection occur in the device user interface?	_____				
MLDP-2.6	Can only manufacturer-authorized persons repair systems when malware has been detected?	_____				
MLDP-2.7	Are malware notifications written to a log?	_____				
MLDP-2.8	Are there any restrictions on anti-malware (e.g., purchase, installation, configuration, scheduling)?	_____				
MLDP-3	If the answer to MLDP-2 is NO, and anti-malware cannot be installed on the device, are other compensating controls in place or available?	_____	__	Section 5.10, MLDP	SI-2	A.12.6.1, A.14.2.2, A.14.2.3, A.16.1.3
MLDP-4	Does the device employ application whitelisting that restricts the software and services that are permitted to be run on the device?	_____	__	Section 5.10, MLDP	SI-3	A.12.2.1
MLDP-5	Does the device employ a host-based intrusion detection/prevention system?	_____	__	Section 5.10, MLDP	SI-4	None
MLDP-5.1	Can the host-based intrusion detection/prevention system be configured by the customer?	_____	__	Section 5.10, MLDP	CM-7	A.12.5.1
MLDP-5.2	Can a host-based intrusion detection/prevention system be installed by the customer?	_____	__	Section 5.10, MLDP		
	NODE AUTHENTICATION (NAUT)			IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
	The ability of the device to authenticate communication partners/nodes.					
NAUT-1	Does the device provide/support any means of node authentication that assures both the sender and the recipient of data are known to each other and are authorized to receive transferred information (e.g. Web APIs, SMTP, SNMP)?	_____	__	Section 5.11, NAUT	SC-23	None
NAUT-2	Are network access control mechanisms supported (E.g., does the device have an internal firewall, or use a network connection white list)?	_____	__	Section 5.11, NAUT	SC-7	A.13.1.1, A.13.1.3, A.13.2.1,A .14.1.3
NAUT-2.1	Is the firewall ruleset documented and available for review?	_____	__			
NAUT-3	Does the device use certificate-based network connection authentication?	_____	__			

	CONNECTIVITY CAPABILITIES (CONN)			IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
	All network and removable media connections must be considered in determining appropriate security controls. This section lists connectivity capabilities that may be present on the device.					
CONN-1	Does the device have hardware connectivity capabilities?	_____	__			
CONN-1.1	Does the device support wireless connections?	_____	__			
CONN-1.1.1	Does the device support Wi-Fi?	_____	__			
CONN-1.1.2	Does the device support Bluetooth?	_____	__			
CONN-1.1.3	Does the device support other wireless network connectivity (e.g. LTE, Zigbee, proprietary)?	_____	__			
CONN-1.1.4	Does the device support other wireless connections (e.g., custom RF controls, wireless detectors)?	_____	__			
CONN-1.2	Does the device support physical connections?	_____	__			
CONN-1.2.1	Does the device have available RJ45 Ethernet ports?	_____	__			
CONN-1.2.2	Does the device have available USB ports?	_____	__			
CONN-1.2.3	Does the device require, use, or support removable memory devices?	_____	__			
CONN-1.2.4	Does the device support other physical connectivity?	_____	__			
CONN-2	Does the manufacturer provide a list of network ports and protocols that are used or may be used on the device?	_____	__			
CONN-3	Can the device communicate with other systems within the customer environment?	_____	__			
CONN-4	Can the device communicate with other systems external to the customer environment (e.g., a service host)?	_____	__			
CONN-5	Does the device make or receive API calls?	_____	__			
CONN-6	Does the device require an internet connection for its intended use?	_____	__			
CONN-7	Does the device support Transport Layer Security (TLS)?	_____	__			
CONN-7.1	Is TLS configurable?					
CONN-8	Does the device provide operator control functionality from a separate device (e.g., telemedicine)?	_____	__			

	PERSON AUTHENTICATION (PAUT)			IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
	The ability to configure the device to authenticate users.					
PAUT-1	Does the device support and enforce unique IDs and passwords for all users and roles (including service accounts)?	_____	__	Section 5.12, PAUT	IA-2	A.9.2.1
PAUT-1.1	Does the device enforce authentication of unique IDs and passwords for all users and roles (including service accounts)?	_____	__	Section 5.12, PAUT	IA-2	A.9.2.1
PAUT-2	Is the device configurable to authenticate users through an external authentication service (e.g., MS Active Directory, NDS, LDAP, OAuth, etc.)?	_____	__	Section 5.12, PAUT	IA-5	A.9.2.1
PAUT-3	Is the device configurable to lock out a user after a certain number of unsuccessful logon attempts?	_____	__	Section 5.12, PAUT	IA-2	A.9.2.1

PAUT-4	Are all default accounts (e.g., technician service accounts, administrator accounts) listed in the documentation?	_____	__	Section 5.12, PAUT	SA-4(5)	A.14.1.1, A.14.2.7, A.14.2.9, A.15.1.2
PAUT-5	Can all passwords be changed?	_____	__	Section 5.12, PAUT		
PAUT-6	Is the device configurable to enforce creation of user account passwords that meet established (organization specific) complexity rules?	_____	__	Section 5.12, PAUT	IA-2	A.9.2.1
PAUT-7	Does the device support account passwords that expire periodically?	_____	__			
PAUT-8	Does the device support multi-factor authentication?	_____	__			
PAUT-9	Does the device support single sign-on (SSO)?	_____	__	Section 5.12, PAUT	IA-2	A.9.2.1
PAUT-10	Can user accounts be disabled/locked on the device?	_____	__	Section 5.12, PAUT	IA-2	A.9.2.1
PAUT-11	Does the device support biometric controls?	_____	__	Section 5.12, PAUT	IA-2	A.9.2.1
PAUT-12	Does the device support physical tokens (e.g. badge access)?	_____	__			
PAUT-13	Does the device support group authentication (e.g. hospital teams)?	_____	__			
PAUT-14	Does the application or device store or manage authentication credentials?	_____	__			
PAUT-14.1	Are credentials stored using a secure method?	_____	__			
	PHYSICAL LOCKS (PLOK)			IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
	Physical locks can prevent unauthorized users with physical access to the device from compromising the integrity and confidentiality of personally identifiable information stored on the device or on removable media					
PLOK-1	Is the device software only? If yes, answer “N/A” to remaining questions in this section.	_____	__	Section 5.13, PLOK	PE- 3(4)	A.11.1.1, A.11.1.2, A.11.1.3
PLOK-2	Are all device components maintaining personally identifiable information (other than removable media) physically secure (i.e., cannot remove without tools)?	_____	__	Section 5.13, PLOK	PE- 3(4)	A.11.1.1, A.11.1.2, A.11.1.3
PLOK-3	Are all device components maintaining personally identifiable information (other than removable media) physically secured behind an individually keyed locking device?	_____	__	Section 5.13, PLOK	PE- 3(4)	A.11.1.1, A.11.1.2, A.11.1.3
PLOK-4	Does the device have an option for the customer to attach a physical lock to restrict access to removable media?	_____	__	Section 5.13, PLOK	PE- 3(4)	A.11.1.1, A.11.1.2, A.11.1.3
	ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CYCLE (RDMP)			IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
	Manufacturer’s plans for security support of third-party components within the device’s life cycle.					
RDMP-1	Was a secure software development process, such as ISO/IEC 27034 or IEC 62304, followed during product development?	_____	__	Section 5.14, RDMP	CM-2	None

RDMP-2	Does the manufacturer evaluate third-party applications and software components included in the device for secure development practices?	_____	__	Section 5.14, RDMP	CM-8	A.8.1.1, A.8.1.2
RDMP-3	Does the manufacturer maintain a web page or other source of information on software support dates and updates?	_____	__	Section 5.14, RDMP	CM-8	A.8.1.1, A.8.1.2
RDMP-4	Does the manufacturer have a plan for managing third-party component end-of-life?	_____	__	Section 5.14, RDMP	CM-8	A.8.1.1, A.8.1.2
	SOFTWARE BILL OF MATERIALS (SBoM)			IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
	A Software Bill of Material (SBoM) lists all the software components that are incorporated into the device being described for the purpose of operational security planning by the healthcare delivery organization. This section supports controls in the RDMP section.					
SBOM-1	Is the SBoM for this product available?	_____	__			
SBOM-2	Does the SBoM follow a standard or common method in describing software components?	_____	__			
SBOM-2.1	Are the software components identified?	_____	__			
SBOM-2.2	Are the developers/manufacturers of the software components identified?	_____	__			
SBOM-2.3	Are the major version numbers of the software components identified?	_____	__			
SBOM-2.4	Are any additional descriptive elements identified?	_____	__			
SBOM-3	Does the device include a command or process method available to generate a list of software components installed on the device?	_____	__			
SBOM-4	Is there an update process for the SBoM?	_____	__			
	SYSTEM AND APPLICATION HARDENING (SAHD)			IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
	The device's inherent resistance to cyber attacks and malware.				CM-7	A.12.5.1*
SAHD-1	Is the device hardened in accordance with any industry standards?	_____	__	Section 5.15, SAHD	AC-17(2)/IA-3	A.6.2.1, A.6.2.2, A.13.1.1, A.13.2.1, A.14.1.2/ None
SAHD-2	Has the device received any cybersecurity certifications?	_____	__	Section 5.15, SAHD	SA-12(10)	A.14.2.7, A.15.1.1, A.15.1.2, A.15.1.3
SAHD-3	Does the device employ any mechanisms for software integrity checking	_____	__			
SAHD-3.1	Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the installed software is manufacturer-authorized?	_____	__			
SAHD-3.2	Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the software updates are the manufacturer-authorized updates?	_____	__	Section 5.15, SAHD	CM-8	A.8.1.1, A.8.1.2

SAHD-4	Can the owner/operator perform software integrity checks (i.e., verify that the system has not been modified or tampered with)?	_____	__	Section 5.15, SAHD	AC-3	A.6.2.2, A.9.1.2, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.1, A.14.1.2, A.14.1.3, A.18.1.3
SAHD-5	Is the system configurable to allow the implementation of file-level, patient level, or other types of access controls?	_____	__	Section 5.15, SAHD	CM-7	A.12.5.1*
SAHD-5.1	Does the device provide role-based access controls?	_____	__	Section 5.15, SAHD	CM-7	A.12.5.1*
SAHD-6	Are any system or user accounts restricted or disabled by the manufacturer at system delivery?	_____	__	Section 5.15, SAHD	CM-8	A.8.1.1, A.8.1.2
SAHD-6.1	Are any system or user accounts configurable by the end user after initial configuration?	_____	__	Section 5.15, SAHD	CM-7	A.12.5.1*
SAHD-6.2	Does this include restricting certain system or user accounts, such as service technicians, to least privileged access?	_____	__	Section 5.15, SAHD	CM-7	A.12.5.1*
SAHD-7	Are all shared resources (e.g., file shares) which are not required for the intended use of the device disabled?	_____	__	Section 5.15, SAHD	CM-7	A.12.5.1*
SAHD-8	Are all communication ports and protocols that are not required for the intended use of the device disabled?	_____	__	Section 5.15, SAHD	SA-18	None
SAHD-9	Are all services (e.g., telnet, file transfer protocol [FTP], internet information server [IIS], etc.), which are not required for the intended use of the device deleted/disabled?	_____	__	Section 5.15, SAHD	CM-6	None
SAHD-10	Are all applications (COTS applications as well as OS-included applications, e.g., MS Internet Explorer, etc.) which are not required for the intended use of the device deleted/disabled?	_____	__	Section 5.15, SAHD	SI-2	A.12.6.1, A.14.2.2, A.14.2.3, A.16.1.3
SAHD-11	Can the device prohibit boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)?	_____	__			
SAHD-12	Can unauthorized software or hardware be installed on the device without the use of physical tools?	_____	__			
SAHD-13	Does the product documentation include information on operational network security scanning by users?	_____	__			
SAHD-14	Can the device be hardened beyond the default provided state?	_____	__			
SAHD-14.1	Are instructions available from vendor for increased hardening?					
SHAD-15	Can the system prevent access to BIOS or other bootloaders during boot?					
SAHD-16	Have additional hardening methods not included in 2.3.19 been used to harden the device?	_____	__			

SECURITY GUIDANCE (SGUD)	IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013

	Availability of security guidance for operator and administrator of the device and manufacturer sales and service.					
SGUD-1	Does the device include security documentation for the owner/operator?	_____	__	Section 5.16, SGUD	AT-2/PL-2	A.7.2.2, A.12.2.1/A .14.1.1
SGUD-2	Does the device have the capability, and provide instructions, for the permanent deletion of data from the device or media?	_____	__	Section 5.16, SGUD	MP-6	A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7
SGUD-3	Are all access accounts documented?	_____	__	Section 5.16, SGUD	AC-6,IA-2	A.9.1.2, A.9.2.3, A.9.4.4, A.9.4.5/A. 9.2.1
SGUD-3.1	Can the owner/operator manage password control for all accounts?	_____	__			
SGUD-4	Does the product include documentation on recommended compensating controls for the device?	_____	__			
	HEALTH DATA STORAGE CONFIDENTIALITY (STCF)			IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
	The ability of the device to ensure unauthorized access does not compromise the integrity and confidentiality of personally identifiable information stored on the device or removable media.					
STCF-1	Can the device encrypt data at rest?	_____	__	Section 5.17, STCF	SC-28	A.8.2.3
STCF-1.1	Is all data encrypted or otherwise protected?					
STCF-1.2	Is the data encryption capability configured by default?					
STCF-1.3	Are instructions available to the customer to configure encryption?					
STCF-2	Can the encryption keys be changed or configured?	_____	__	Section 5.17, STCF	SC-28	A.8.2.3
STCF-3	Is the data stored in a database located on the device?	_____	__			
STCF-4	Is the data stored in a database external to the device?	_____	__			
	TRANSMISSION CONFIDENTIALITY (TXCF)			IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
	The ability of the device to ensure the confidentiality of transmitted personally identifiable information.					
TXCF-1	Can personally identifiable information be transmitted only via a point-to-point dedicated cable?	_____	__	Section 5.18, TXCF	CM-7	A.12.5.1
TXCF-2	Is personally identifiable information encrypted prior to transmission via a network or removable media?	_____	__	Section 5.18, TXCF	CM-7	A.12.5.1
TXCF-2.1	If data is not encrypted by default, can the customer configure encryption options?	_____	__			
TXCF-3	Is personally identifiable information transmission restricted to a fixed list of network destinations?	_____	__	Section 5.18, TXCF	CM-7	A.12.5.1
TXCF-4	Are connections limited to authenticated systems?	_____	__	Section 5.18, TXCF	CM-7	A.12.5.1
TXCF-5	Are secure transmission methods supported/implemented (DICOM, HL7, IEEE 11073)?	_____	__			

				IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
	TRANSMISSION INTEGRITY (TXIG)					
	The ability of the device to ensure the integrity of transmitted data.					
TXIG-1	Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission?	_____	__	Section 5.19, TXIG	SC-8	A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3
TXIG-2	Does the device include multiple sub-components connected by external cables?	_____	__			

				IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
	REMOTE SERVICE (RMOT)					
	Remote service refers to all kinds of device maintenance activities performed by a service person via network or other remote connection.					
RMOT-1	Does the device permit remote service connections for device analysis or repair?	_____	__		AC-17	A.6.2.1, A.6.2.2, A.13.1.1, A.13.2.1, A.14.1.2
RMOT-1.1	Does the device allow the owner/operator to initiative remote service sessions for device analysis or repair?	_____	__			
RMOT-1.2	Is there an indicator for an enabled and active remote session?	_____	__			
RMOT-1.3	Can patient data be accessed or viewed from the device during the remote session?	_____	__		AC-17	A.6.2.1, A.6.2.2, A.13.1.1, A.13.2.1, A.14.1.2
RMOT-2	Does the device permit or use remote service connections for predictive maintenance data?	_____	__			
RMOT-3	Does the device have any other remotely accessible functionality (e.g. software updates, remote training)?	_____	__			

				IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
	OTHER SECURITY CONSIDERATIONS (OTHR)					
	NONE					
	Notes:					
Note 1	Example note. Please keep individual notes to one cell. Please use separate notes for separate information					

Documento Firmato Digitalmente

AS FO
Azienda sanitaria
Friuli Occidentale

REGIONE AUTONOMA FRIULI VENEZIA GIULIA

Determinazione n. 145 del 11/02/2026

CERTIFICATO DI PUBBLICAZIONE

La presente determinazione viene pubblicata nell'albo pretorio dell'Azienda Sanitaria Friuli Occidentale, per quindici giorni consecutivi dal 12/02/2026, ai sensi dell'art.32, c.l, della Legge n.69 del 18.06.2009.

CERTIFICATO DI ESECUTIVITA'

La presente determinazione è divenuta esecutiva in data 12/02/2026, ai sensi dell'art.50, della L.R. n.49 del 19.12.1996.

Il presente provvedimento verrà trasmesso al Collegio Sindacale (art. 3, D.Lgs. 502/92 e successive modificazioni).

Ufficio Proponente: APPROVVIGIONAMENTI E GESTIONE CONTRATTI BENI E SERVIZI

Inviato per quanto di competenza a:

ASSISTENZA FARMACEUTICA
DIREZIONE SANITARIA
PROGRAMMAZIONE E CONTROLLO
APPROVVIGIONAMENTI E GESTIONE CONTRATTI BENI E SERVIZI
DIREZIONE MEDICA OSPEDALIERA SAN VITO AL T. - SPILIMBERGO
DIREZIONE MEDICA OSPEDALIERA PORDENONE - SACILE
INGEGNERIA CLINICA
GESTIONE ECONOMICO FINANZIARIA E FISCALE

Il funzionario incaricato
Matteo Bordin
Firmato digitalmente

Data 12/02/2026

Elenco firmatari

ATTO SOTTOSCRITTO DIGITALMENTE AI SENSI DEL D.P.R. 445/2000 E DEL D.LGS. 82/2005 E SUCCESSIVE MODIFICHE E INTEGRAZIONI

Questo documento è stato firmato da:

NOME: MATTEO BORDIN
CODICE FISCALE: BDRMTT90L02F770Z
DATA FIRMA: 12/02/2026 08:07:46
IMPRONTA: 8D7FEA7D4D13CD1C68F8FF1165FF9F4D0749910B5A8A450808BADD35D5267B71
0749910B5A8A450808BADD35D5267B716F797DFB3225A0CCFD12FF7D4EE4F64A
6F797DFB3225A0CCFD12FF7D4EE4F64A663D06B5F5C6AEF6207258A44EEF03A8
663D06B5F5C6AEF6207258A44EEF03A85C394420B2DB27A4D71100273A883378