IT-vereisten voor PC ’s, Serversoftware, medische toestellen en randapparatuur in het kader van een bestek

Voor alle bijkomende vragen i.v.m. dit document kunt u terecht bij de verantwoordelijke van dit document.

Inhoud

1 TECHNISCHE VEREISTEN 4

1.1 Clients 4

1.1.1. Hardware 4
1.1.2. Software 4
1.1.3. Randapparatuur 5
1.1.4. Mobiele apparaten 5

1.2 On Site Hosted 6

1.2.1. Server 6
1.2.2. Database 7
1.2.3. Opslag & Backup 7
1.2.4. Security 7
1.2.5. Monitoring 8
1.2.6. Remotely Hosted/Software as a Service 8
1.2.7. Identity and access management (IAM) 8
1.2.8. IT Security 9
1.2.9. Status applicatie 9

1.3 Netwerk 9

1.3.1. Authenticatie & segmentatie 9
1.3.2. Wired 10
1.3.3. WIFI 10

1.4 Inloggen, gebruikersbeheer 10

1.4.1. Authenticatie: 10
1.4.2. Authorisatie 11
1.4.3. Rollen 11
1.4.4. Opzet gebruikersbeheer 11

1.5 Koppelingen 12

1.5.1. Algemeen 12
1.5.2. Medische beeldvorming 13
1.5.3. Context switchen 13

1.6 Artificiële Intelligentie: minimale richtlijnen 13

1.6.1. Gebruik van het AI in het ziekenhuis 13
1.6.2. Algemene richtlijnen 13
1.6.3. Specifieke richtlijnen: trainen van een AI-model 13

2 ONDERHOUD EN ONDERSTEUNING 14

2.1 Remote support 14

2.2 Change- en Releasemanagement 14

2.3 Onderhoudscontract 15

2.4 Business Continuity 15

3 DOCUMENTATIE EN OPLEIDINGEN 16

3.1 Architectuur 16

3.2 Documentatie 16

1 TECHNISCHE VEREISTEN

1.1 Clients

1.1.1. Hardware

De hardware wordt door het ziekenhuis aangekocht volgens het standaard hardware aanbod. Alle nodige hardware specificaties voor het vlot werken van de toepassing worden duidelijk vermeld.

In uitzonderlijke gevallen kan de hardware door de leverancier geleverd worden. Dit enkel na overleg met de IT-afdeling van het ziekenhuis. Voor PC's en laptops dient er een minimum van 8GB werkgeheugen en een SSD schijf van minimaal 256GB in het toestel aanwezig te zijn. Schermen zijn minimaal 24 inch en High Definition (1920x1080p). Processor is minimaal I5 12th Gen.

Het aantal vereiste usb-poorten en/of uitbreidingskaarten dienen vermeld te worden in de offerte.

Client computers worden wired geconnecteerd wanneer het een desktop of printer betreft en wireless wanneer het een laptop, tablet of telefoon betreft.

1.1.2. Software

Alle PC-toepassingen moeten draaien op Windows 11 Enterprise 64-bit Nederlandstalig. Alle uitzonderingen worden op voorhand met de IT-dienst besproken. Bv. Gebruik van long term build,… .

Geef expliciet aan of de softwarecomponenten kunnen draaien in een gevirtualiseerde omgeving. (Vmware Horizon)

Clients worden altijd toegevoegd aan het domein van het ziekenhuis (geen werkgroep-pc's). Dit is ook het geval wanneer de client hardware door de leverancier geleverd wordt. Hierdoor krijgen deze toestellen ook de standaard policies die bepaald zijn.

Opdat alle toestellen dezelfde tijd zouden hebben, is het van noodzakelijk dat het device ofwel lid is van het Active Directory domein (typisch voor PC's en laptops), ofwel z'n klok synchroniseert met een centrale, interne NTP-server. In het Jan Yperman wordt hiervoor de primary domain controller gebruikt.

Alle software moet werken onder een persoonlijk gebruikersaccount. Indien op bepaalde mappen extra rechten nodig zijn, moet dit vooraf gedetailleerd vermeld worden. Volledige administratorrechten worden in geen enkel geval toegestaan!

Clientsoftware is bij voorkeur webbased (3-tier) of een client – server configuratie. Web based toepassingen moeten draaien onder de hoogste versie van Microsoft Edge. Andere browsers worden niet ondersteund of geïnstalleerd op de client computer. Er wordt gebruik gemaakt van het https protocol. Het certificaat hiervoor, gebruikt TLS1.2

Data lokaal opslaan op de client wordt niet toegestaan. Hiervoor kan eventueel een netwerkshare toegekend worden. Echter dient men hiervoor een schatting te maken van de periodieke groei van deze data. De data moet het toelaten een archivering hierop te kunnen uitvoeren.

De installatie van de software – nieuw of upgrades – gebeurt met behulp van Microsoft System Center. De leverancier voorziet hiervoor een MSI-pakket en een gedetailleerde installatieprocedure, waarin ook beschreven wordt welke software afhankelijkheden nodig zijn.

Op alle clients worden frequent (maandelijks) de kritische Windows-updates geïnstalleerd. We volgen hierbij het patchbeleid van Microsoft en proberen om nooit meer dan 2 patches achter te zitten. De applicatie/geïnstalleerde software op cliënts mag niet verhinderen dat we kritische Windows patches niet kunnen uitvoeren.

De software moet steeds compatibel zijn met de nieuwste patches. Het is immers niet mogelijk om voor de client computers een uitzondering te maken, zodat zij bepaalde updates niet zouden krijgen.

Op Clients wordt voor de beveiliging gebruik gemaakt van Microsoft Defender XDR en Bitlocker. Deze kunnen in geen geval afgezet worden. Specifieke map of bestand exclusies moeten vooraf afgesproken worden, alsook het gebruik van vertrouwde bestanden.

Op alle clients wordt Windows firewall geactiveerd. Indien bepaalde poorten geopend moeten worden, moet dit vooraf duidelijk vermeld worden. Ook toegang tot het internet op standaard of unieke poorten moet afgesproken en gedocumenteerd zijn.

Indien voor rapportering, databasekoppeling,… software op de client aanwezig dient te zijn (Acrobat, Word, Excel, Oracle clients,..) wordt dit ook opgenomen in de specificaties. Deze kan eventueel geïnstalleerd worden mits deze geen conflicten oplevert met de bestaande toepassingen op de client. Patching van deze software volgt gelijke voorwaarden als het Operating System.

De standaarden binnen het ziekenhuis (service packs, officeversie, browser, javaversie …) worden gerespecteerd en vooraf samen met de klant besproken en indien nodig uitgetest.

Toepassingen kunnen enkel extern worden aangeboden via VDI Horizon.

1.1.3. Randapparatuur

Alle printers worden via het netwerk aangesloten en geïnstalleerd op een printserver. Op de printserver wordt steeds gewerkt met universele drivers. Uitzonderingen kunnen enkel na overleg en akkoord van de IT dienst van het Jan Yperman ziekenhuis!

Wanneer (barcode)scanners noodzakelijk zijn, moeten de specificaties hiervan vooraf duidelijk vermeld worden. Ook de (barcode)scanners worden bij voorkeur via het ziekenhuis aangekocht in functie van standaardisatie.

1.1.4. Mobiele apparaten

Voor mobiele apparaten (smartphones, tablets, …) bieden wij een MDM Workspace One Unified Endpoint Management (Airwatch) omgeving aan voor iOS en Android. Dit om apps op de mobiele toestellen te beheren en te voorzien van extra beveiliging binnen het Jan Yperman Ziekenhuis netwerk. Jan Yperman Ziekenhuis beheert het business gedeelte van het mobiele toestel en heeft de mogelijkheid om dit gedeelte remote te verwijderen.

De minimum ondersteunde versie van Android is steeds de laatst beschikbare – 3 versies. Voor IOS is dit tevens de laatste beschikbare -3 versies.

Indien de toestellen gebruik maken van onze WIFI netwerk dienen de toestellen binnen het Jan Yperman getest te worden qua connectiviteit, roaming, enz.. tijdens de offerte faze van de aanbesteding. Bij voorkeur is het ook beter om meerdere toestellen te testen om te zien welke het best scoort.

1.2 On Site Hosted

1.2.1. Server

De servertoepassing dient bij voorkeur te draaien op Windows 2022 met de laatste updates binnen een VMWare ESX 8.0.2 (en hoger) omgeving (virtualisatie). Het ziekenhuis voorziet in de nodige hardware. Hiervoor dient geen hardware te worden opgenomen in het voorstel.

De leverancier voorziet eveneens dat zijn software steeds gesupporteerd blijft op de laatste versie van windows. Als toestel lid is van het domain dan wordt deze automatisch gesynced met de interne NTP-server. Indien de support op een windowsversie dreigt te vervallen zal het Jan Yperman ziekenhuis contact opnemen met de leverancier om de applicatie te migreren naar een gesupporteerde versie. Kosten voor dergelijke migraties zijn ten laste van de leverancier.

Ook voor serversystemen anders dan windows (unix, linux, kubernetes, …) voorziet de leverancier regelmatige in updates.

Vermits het om een virtuele omgeving gaat, zijn er geen USB- en seriële aansluitingen mogelijk. hardwaredongels kunnen met andere woorden niet gebruikt worden voor licentieredenen.

De leverancier zorgt voor de nodige certificering van de hardware – software compliance.

De architectuur wordt in detail omschreven, indien gebruik wordt gemaakt van meerdere servers (vb. application, database, webserver, linkserver enz.) worden die individueel gespecificeerd. Jan Yperman Ziekenhuis wenst ook over een test- en/of een opleidingsomgeving te beschikken en vraagt ook hiervoor de details. De test- en opleidingslicenties zijn inbegrepen in de prijs.

De leverancier zorgt voor een **exacte** omschrijving van de specificaties van de nodige hardware m.a.w. aantal virtuele processoren, grootte geheugen, schijfcapaciteit, enz., volledig gedetailleerd.

We verwachten een optimale performantie. Jan Yperman Ziekenhuis verwacht een responstijd m.b.t. de interactieve software van minder dan 1 seconde. De leverancier geeft duidelijk aan wanneer en voor welke acties dit niet kan gegarandeerd worden.

Op de server mogen er geen applicaties op de desktop actief zijn. Dit om te beletten dat er altijd aangemeld moet zijn op de server.

Het overnemen van een server gebeurt via RDP of SSH (geen vSphere cliënt). Gebruik de server niet als cliënt. Hiervoor kan het Jan Yperman Zieken een (virtueel) werkstation voorzien.

De leverancier geeft aan welke additionele licenties nodig zijn (bv operating systems, application servers, databasesoftwares) om de software te installeren en draaien.

Er mag enkel met software license sleutels egwerkt worden. Het gebruik van hardware USB Dongles is niet toegestaan.

1.2.2. Database

Bij gebruik van databases wordt de voorkeur gegeven aan MS SQL Server (minimaal versie 2022). Het Jan Yperman Ziekenhuis beschikt over een allways-on SQL-server cluster. Oracle wordt enkel getolereerd indien embedded en bij licentie audits vallen alle mogelijke kosten die daaruit voortvloeien ten laste van de inschrijver. Er wordt vooraf duidelijk vermeld met welke versies en servicepacks kan worden gewerkt. Bij wijziging wordt de klant hier vooraf van verwittigd en ondersteund. De versie/servicepack heeft nog mainstream support bij de desbetreffende firma.

Initiële tuning van de SQL-server database gebeurt door de leverancier. Onderhoud van de SQL-Server database wordt voorzien door Jan Yperman Ziekenhuis. De leverancier kan enkel database-eigenaar zijn van hun eigen databases en geen system administrator van de SQL omgeving.

1.2.3. Opslag & Backup

De gegevens worden bewaard op de centrale storage van het ziekenhuis, de sizing wordt onderverdeeld in:

- Operating System
- Software componenten (aparte drive)
- Index - logfiles
- Data
- …

De leverancier geeft aan welke de totale ruimte nodig is voor de opslag. Deze wordt gegeven op basis van behoefte voor het eerste jaar en de te verwachten jaarlijkse aangroei. Indien de toepassing logging wegschrijft, wordt dit meegedeeld incl. hoeveelheid, locatie, en hoe deze na verloop van tijd te verwijderen.

Afhankelijk van de eigen behoeftes beslist de klant hoeveel jaar hij de data online houdt. Er wordt een vlotte archivering van oudere gegevens voorzien. Archivering moet mogelijk zijn op jaarlijkse basis. De online werking mag hierdoor niet verstoord worden. Het archief moet op een vlotte manier consulteerbaar zijn. Er moet duidelijk vermeld worden op welke manier de archivering zal gebeuren en welke benodigde schijfruimte (of ander medium) hiervoor dient voorzien te worden.

Jan Yperman Ziekenhuis zorgt voor een regelmatige back-up van de data, centraal geregeld via het product Rubrik Het principe is back-up to disc (met deduplicatie). Andere/eigen vormen van backup zijn enkel toegestaan na overleg met de IT dienst van het Jan Yperman ziekenhuis.

Er worden enerzijds image back-ups genomen d.m.v. integratie met VMware. Dit betekent dat de oplossing overweg kan met VMware snapshots.
Anderzijds moet het ook mogelijk zijn om online back-ups te nemen via een back-up agent. Dit wil zeggen dat er geen downtime is van de applicatie voor het nemen van consistente backups.

De leverancier vermeldt welke data belangrijk is om op te nemen in de back-up.

1.2.4. Security

Servers zijn ‘hardened’ volgens de aanbevelingen van CIS (centre of internet security), Microsoft.

Op alle windows servers worden frequent de kritische Windows-updates geïnstalleerd. We volgen hierbij het patchbeleid van Microsoft. De applicatie/geïnstalleerde software op servers mag niet verhinderen dat we kritische Windows patches niet kunnen uitvoeren.

Op alle servers (ook niet windows) wordt Microsoft Defender end point protection for servers geïnstalleerd. Deze kan/mag in geen geval afgezet worden. Er kunnen wel bestanden/mappen uitgesloten worden van scanning. De installatie van Defender wordt bij voorkeur uitgevoerd door de IT dienst van het ziekenhuis. De nodige licenties zijn aanwezig in het ziekenhuis.

Op alle windows servers wordt Windows firewall geactiveerd. Indien bepaalde poorten geopend moeten worden, moet dit vooraf duidelijk vermeld worden.

Alle beheerstaken dienen uitgevoerd te worden via beveiligde kanalen (SSH, https, …). Gebruik certificaten gebaseerd op minimaal TLS 1.2.

Vermijd standaard wachtwoorden. Dit is een vereiste! Paswoorden dienen aangepast te worden volgens de best practices, volgens de wachtwoord-procedure. Wachtwoorden dienen gekend te zijn bij ICT.

1.2.5. Monitoring

De leverancier voorziet in monitoring van de oplossing. Indien geen monitoring kan voorzien worden wordt duidelijk beschreven welke componenten op welke manier gemonitord moeten worden.

1.2.6. Remotely Hosted/Software as a Service

De kandidaat-leverancier, wanneer die zijn product of dienst aanbiedt via een “cloud”-gebaseerd systeem (hiermee bedoelen we dat de dataverwerking deels of volledig buiten de infrastructuur van het ziekenhuis gebeurt), bevestigt zich in lijn te stellen met de GDPR richtlijnen (AVG).
Het ziekenhuis kan aan de leverancier vragen om een ‘vragenlijst leveranciersbeoordeling informatieveiligheid’ in te vullen, vóór het afsluiten van de overeenkomst.

Daarnaast voorziet de leverancier in een exit-strategie (bij einde contract) zodat de applicatiedata in een af te spreken standaard formaat terug ter beschikking gesteld kan worden aan het Jan Yperman ziekenhuis.

1.2.7. Identity and access management (IAM)

De kandidaat leverancier zorgt ervoor dat de in de cloud gehoste applicatie integreert met imprivata single sign on of ***bij voorkeur*** met Azure Active Directory (Microsoft Entra) op de tenant van het ziekenhuis. Het Jan Yperman Ziekenhuis wil gebruik maken van authenticatie t.o.v. zijn eigen domein.

Indien de in de cloud gehoste applicatie eveneens van buiten het ziekenhuisnetwerk consulteerbaar is, dient multifactor authenticatie voorzien te worden aan de hand van Microsoft authenticator (standaard MFA oplossing voor alle toepassingen binnen het ziekenhuis omwille van eenvoud voor de eindgebruiker). Bij integratie met Microsoft Entra wordt MFA aangeboden vanuit de Microsoft 365 tenant van het ziekenhuis. Elke afwijking op bovenstaande dient vooraf met de ICT dienst besproken en door de ICT dienst geëvalueerd te worden.

De kandidaat-leverancier werkt te allen tijde met door een erkend Certificate authority afgeleverde geldige certificaten.

1.2.8. IT Security

Data security moet worden uitgevoerd op volgende niveaus:

- Device level
- Transport level
- At rest, remotely of on premise

Hierbij wordt de data geëncrypteerd.

De leverancier is verantwoordelijk voor het beschermen van z'n eigen infrastructuur en geeft mee welke maatregelen er naast de vereiste installatie van Microsoft defender nog van toepassing zijn.

De leverancier zorgt dat data van het Jan Yperman Ziekenhuis niet toegankelijk is voor andere klanten. De leverancier verduidelijkt aan het Jan Yperman Ziekenhuis op welke manieren dit wordt uitgevoerd.

De leverancier rapporteert steeds alle gekende vulnerabilities en security issues met de software (on-premise en/of Cloud) en de remediëring om de vulnerabilities weg te werken.

Het Jan Yperman Ziekenhuis verwacht dat de leverancier die persoonsgegevens verwerken en die bedrijfskritische applicaties (incl. informatie- en netwerksystemen) aanleveren, bij voorkeur over een ISO 27001 certificaat beschikt of aantoont dat het volgens de geest van de ISO 27001 standaarden te werken. Het Ziekenhuis accepteert ook CyFun certificatie.
Het ziekenhuis kan aan elke leverancier vragen om een 'vragenlijst leveranciersbeoordeling informatieveiligheid' in te vullen, vóór het afsluiten van de overeenkomst.

1.2.9. Status applicatie

De leverancier biedt mogelijkheden om de status door te geven van de applicatie aan het Jan Yperman Ziekenhuis. Jan Yperman Ziekenhuis wordt te allen tijde ruim op voorhand op de hoogte gebracht bij onderbrekingen van de applicatie. (Zowel gepland als ongepland). Dit om de interne ITSM processen te bewerkstelligen.

1.3 Netwerk

1.3.1. Authenticatie & segmentatie

Het toestel dient het 802.1x protocol te ondersteunen om toegang te krijgen tot het interne netwerk. Authenticatie gebeurt door een radiusserver op basis van het MAC-adres of via Active Directory.

Enkel gekende toestellen worden op het netwerk toegelaten. Dit betekent ook dat laptops van derden niet toegelaten zijn op het productienetwerk. Eveneens kan er via het guest-netwerk tijdelijk internettoegang voorzien worden.

Jan Yperman Ziekenhuis gebruikt VLAN segmentatie. Deze worden dynamisch toegekend via een radiusserver.

Alle devices (vb printers, Medical, ea...) die op het netwerk worden aangesloten moeten het principe van het huidig IP plan volgen.

1.3.2. Wired

Het netwerk is verdeeld in L3 segmenten o.a. volgens de locatie in het gebouw. Elk knooppunt heeft dus unieke subnets. Toestellen moeten routering (Layer 3) ondersteunen. Multicast of L2 UPNP is niet mogelijk.

De poorten van de switches staan op auto-negotiate. Netwerksnelheid en duplex mode moeten dus automatisch gedetecteerd worden.

Een netwerkdevice moet z'n IP-adres aanvragen via het DHCP protocol en moet DNS gebruiken om connectie te leggen met andere systemen. Reservatie van IP-adressen is enkel mogelijk voor het bekabeld netwerk en na akkoord van de IT dienst van het Jan Yperman ziekenhuis.

De leverancier vermeldt welke en hoeveel netwerk- of andere aansluitingen er nodig zijn voor pc's, printers, koppeling toestellen, enz … Hij geeft tevens op of Power over Ethernet noodzakelijk is (PoE) en welke wattages nodig zijn.

1.3.3. WIFI

Dekking is voorzien over gans het ziekenhuis en gevalideerd geweest voor laptops, Location Based Services en WiFi Telefonie. Door de hoge densiteit van Access Points wordt er door toestellen frequent geroamed. De applicatie moet dus overweg kunnen met korte onderbrekingen omwille van roaming. Idealiter wordt de roaming vooraf getest.

Een toestel moet 5ghz ondersteunen, met WPA2-AES.

Volgende SSID's worden voorzien:

- *JYZ-Intern*: 802.1x authenticatie via radius server
- JYZ-Intern-PSK: MAC authenticatie via radius server, enkel toegang intern netwerk

Een netwerkdevice moet z'n IP-adres aanvragen via het DHCP protocol en moet DNS gebruiken om connectie te leggen met andere systemen Afhankelijk van de authenticatie zal de gebruiker een IP adres krijgen uit een bepaald subnet en eventueel afscheiding aan de hand van een Firewall.

Reservaties van IP-adressen op het wireless netwerk is niet mogelijk.

1.4 Inloggen, gebruikersbeheer

Het ziekenhuis heeft vandaag een eigen directoryserver die we als centraal punt voor user-beheer wensen te gebruiken. De aangeboden oplossing dient geïntegreerd te zijn met Microsoft Active Directory (Windows 2019 schema objectversion 88)

De koppeling met AD is een minimumvereiste.

1.4.1. Authenticatie:

- Gebruikers dienen zich te authenticeren door ingave van een gebruikersnaam en paswoord op het aanmeldscherm. Deze 2 velden, als ook de bevestigingsknop en annuleringsknop zijn

op het aanmeldscherm onmiddellijk beschikbaar (dus niet verborgen totdat bepaalde velden ingevuld zijn). Op het aanmeldscherm zijn geen andere keuzes voorhanden. Dit o.a. ten behoeve van een Fast User Swiching systeem.

- Authenticatie gebeurt t.o.v. Microsoft Active Directory (AD).
- Gebruikersnamen zijn uniek, volgen de conventie van AD (o.a. lengte) en zijn niet case sensitive.
- Wachtwoorden volgen het wachtwoordbeleid van Jan Yperman Ziekenhuis. Belangrijk hierbij is dat het wachtwoord minimaal 12 karakters met microsoft complexity moet bevatten en dit kunnen vreemde tekens zijn. Het wachtwoord moet regelmatig gewijzigd worden.
- Inloggen dient individueel te gebeuren. Alle acties worden opgeslagen met de unieke gebruikerscode.
- Idealiter voorziet de applicatie de mogelijkheid tot automatische logout na een vooraf bepaalde tijd.
- Indien SSO (Single Sign On) gewenst is, dan dient dit door de toepassing ondersteund te worden. Hierbij moet SSO geactiveerd/gedeactiveerd kunnen worden voor bepaalde groepen van gebruikers.
- Wisselen van een gebruiker kan gebeuren zonder de applicatie volledig af te sluiten en opnieuw op te starten.

1.4.2. Authorisatie

1.4.3. Rollen

- Hoewel het systeem gebruik dient te maken voor authenticatie van Microsoft Active Directory dient het een beheermodel te omvatten voor gebruikers en groepen en rollen waarin de mogelijkheid bestaat authorisatie te voorzien op rollen/groepen/gebruikers. De voorkeur is steeds role based access. De gebruikers hebben een set van rechten die hen al dan niet toegang zullen geven tot specifieke functionaliteiten binnen het software systeem.
- De volgende rollen moeten minimaal gedefinieerd kunnen worden en zullen verder in dit document gebruikt worden:
    1. Key-users: volledige toegang: Uitgebreide rechten binnen het systeem. Een Key User heeft de mogelijkheid om nieuwe gebruikers aan te maken en is verantwoordelijk voor het rechtenbeheer. Tevens dient de Key Users als vraagbaak voor overige users. Mocht de Key User de vraag niet kunnen beantwoorden kan deze middels het supportsysteem een vraag indienen voor ondersteuning.
    2. ICT :het geleverde platform kunnen ondersteunen, dit onderverdeeld in applicatief beheer, helpdesk en systeembeheer.
- Er dienen aangepaste toegangsrechten mogelijk te zijn tot op individueel niveau
- De leverancier beschrijft hoe rollen worden beheerd binnen de software. Voorkeur is Active directory based

1.4.4. Opzet gebruikersbeheer

Het huidige gebruikersbeheer van Jan Yperman Ziekenhuis is opgezet in Active Directory.

Bij de koppeling met gebruikersbeheer dient de rol meegegeven te worden. Met rol bedoelen we: welke rechten een gebruiker krijgt, welke menupunten/tabbladen zichtbaar zijn, vb van rollen: arts, verpleegkundigen, apotheekgebruikers.

Opvragen van de rollen van een gebruiker gebeurt:

- Rechtstreeks in AD, rollen worden bepaald door security groepen. Het beheer van de gebruikers en rollen gebeurt in AD.
- Door HL7 PMU berichten via Mirth. Het is mogelijk om rol en context (dienst/discipline) mee te geven.
- Dan wel via file synchronisatie. Zie lager
- Indien de leverancier geen van beide mogelijkheden kan aanbieden, dan stelt de leverancier voor op welke manier hij integreert met onze Active directory.

Indien gewerkt wordt met file synchronisatie gebeurt dit op deze manier:

- Het bestand wordt afgeleverd in een directory lokaal door ons afgesproken en bereikbaar via netwerkshare
- Per wijziging wordt 1 bestand geleverd
- Naam van het bestand bevat de datum van verwerking en heeft als extensie txt
- De verwerking gebeurt in real-time

Logging:

- Het systeem zorgt voor logging van de verwerking en eventuele foutmeldingen.
- Deze logging is door ons raadpleegbaar.

1.5 Koppelingen

1.5.1. Algemeen

De architectuur van het systeem dient open te zijn zodat de integratie met de rest van de ziekenhuisapplicaties steeds kan worden gegarandeerd. Anderzijds moet gegarandeerd worden dat medische toestellen blijven werken bij het uitvallen van het netwerk en/of het EAI-platform.

Het uitwisselen van informatie tussen, of aanroepen van services van de toepassingen dient te gebeuren via de in het ziekenhuis gebruikte Mirth-applicatie. Het beheer van dit EAI-platform (Enterprise Application Integration) wordt door het Jan Yperman Ziekenhuis gedaan.

Binnen Jan Yperman Ziekenhuis gebruiken we de HL7 (Health Level Seven) standaardtaal om elektronische gezondheids- en patiëntinformatie te delen en te integreren.

Indien van toepassing dan moeten deze koppelingen ook gerealiseerd worden:

- Patiëntkoppeling (HL7 ADT versie 2.3)
    - Liefst voorzien we een ADT query interface met bevraging via PatientID of VisitID.
- Artsenkoppeling (HL7 MFN)
- Resultatenkoppeling (Medisch dossier – HL7 ORU)
- Administratieve koppeling

- Logistieke koppeling

1.5.2. Medische beeldvorming

Het toestel voor medische beeldvorming moet voorzien zijn van een interfacemogelijkheid naar de PACS (PacsOnWeb) en dit volgens de DICOM standaarden. Volgende standaarden dienen voorzien te zijn :

- Dicom Store
- Dicom Modality Worklist
- Dicom Query/Retrieve

De configuratie van de Dicom functionaliteit op de toestellen door de leverancier moet deel uitmaken van het voorstel. Configuratie aan de kant van de PACS neemt het ziekenhuis op met de PACS leverancier. Hierbij moeten de nodige documentatie, tools en toegangsrechten worden voorzien door zowel de leverancier van het toestel als de leverancier van het PACS zodat het ziekenhuis zelf in staat is om de koppelingen te realiseren zonder verdere tussenkomst van de leverancier.

Voor de DICOM configuratie wordt minimaal 4 weken op voorhand contact opgenomen met de IT-dienst. Tevens wordt alle technische documentatie bij de offerte gevoegd.

1.5.3. Context switchen

We bieden de mogelijkheid om vanuit een toepassing een andere toepassing op te starten, zonder dat de gebruiker zich opnieuw moet authentiseren. Context wordt meegegeven (loginnaam en patiënt). Het paswoord wordt niet meegeleverd. Om dit op een veilige manier te laten gebeuren werken we met een token die beperkt in tijd kan gebruikt worden.

1.6 Artificiële Intelligentie: minimale richtlijnen

1.6.1. Gebruik van het AI in het ziekenhuis

Zowel bij zorg als administratieve toepassing blijft AI steeds een hulpmiddel, d.w.z. dat de tool op geen enkele wijze een automatische diagnose of beslissing mag nemen die een grote impact heeft op de betrokkene (o.a. profiling of een besluit waaraan rechtsgevolgen verbonden zijn), zonder menselijke tussenkomst.

1.6.2. Algemene richtlijnen

Indien datasets worden doorgegeven aan een leverancier (= de ontwikkelaar van het algoritme) en de data hierdoor de omgeving van het ziekenhuis verlaten, dan wordt er maximaal ingezet op anonimisering of pseudonimisering van de data.
Met anonimiseren bedoelen we dat geen enkele partij (zowel het ziekenhuis als de leverancier) de data kan linken aan een patiënt.
Indien anonimiseren niet het geval is, moet de leverancier altijd de verwerkersovereenkomst van het ziekenhuis ondertekenen.

De aangeleverde datasets moeten ten allen tijde binnen de E.E.R. blijven, tenzij het land beschikt over een adequaatheidsbesluit van de E.U. of de Standard Contractual Clauses ondertekent.

Indien anonimisering of pseudonimisering niet mogelijk is, dan moet er vooraf een DPIA opgemaakt worden om de privacy risico's in kaart te brengen.

Bij de verwerking van (identificeerbare) patiëntengegevens moet de leverancier aantonen te voldoen aan de basisprincipes van de AI-Act: data minimalisatie, data protection by design en data security. Het ziekenhuis kan aan de leverancier vragen om een 'Vragenlijst voor toepassingen en projecten met AI component' in te vullen, vóór het afsluiten van de overeenkomst.

1.6.3. Specifieke richtlijnen: trainen van een AI-model

Het trainen van algoritmes bij medische hulpmiddelen en digitale gezondheidsapplicaties en de ontwikkeling van innovatieactiviteiten in het ziekenhuis, vallen onder de toegestane doelstellingen van de European Health Data Space.

Indien hierbij (identificeerbare) persoonsgegevens betrokken zijn, dan baseert het ziekenhuis zich op de rechtsgrond van wetenschappelijk onderzoek om kwaliteitsvolle zorg aan te bieden. Indien het trainen van het algoritme niet gebeurt binnen de tenant van het ziekenhuis, zijn de basisprincipes van anonimisering en pseudonimisering van toepassing.
De aangeleverde data waarmee het AI-model getraind wordt, blijft eigendom van het Jan Yperman Ziekenhuis en mag door de leverancier niet voor andere doeleinden gebruikt worden.

Indien de data voor de leverancier noodzakelijk blijkt voor de verdere ontwikkeling van het algoritme, dan kan dit enkel met geanonimiseerde datasets.

2 ONDERHOUD EN ONDERSTEUNING

2.1 Remote support

Voor support en onderhoud van op afstand bieden we standaard 2 mogelijkheden aan:

- Een remote sessie via SSLVPN. De toegang is beveiligd met een eID of RSA-token en minimaal 2-factor authenticatie.
- De leverancier is ermee akkoord dat in de toekomst eerst expliciet toegang dient aangevraagd te worden bij de IT dienst (of andere dienst) van het Jan Yperman ziekenhuis vooraleer een connectie kan opgezet worden.
- De leverancier is ermee akkoord dat in de toekomst alle remote sessie worden opgenomen (session recording) om audit redenen.

2.2 Change- en Releasemanagement

Binnen Jan Yperman Ziekenhuis werken we met een Change and Release (ITIL) aanpak, voor ons moet het duidelijk zijn hoe de kandidaat-leverancier omgaat met preventief, correctief, evolutief onderhoud, updates en upgrades.

Onderstaande is een niet-exhaustieve lijst die door de kandidaat-leverancier dient te worden aangevuld in functie van zijn eigen servicemodel.

- Frequentie: om de hoeveel tijd is een update/upgrade te verwachten?
- Productie disruptie: kan een update/upgrade uitgevoerd worden tijdens productie of dient hiervoor de oplossing tijdelijk offline worden gezet?
- Gebeurt de installatie van nieuwe versies eerst op een testplatform?
- Wordt versie-beheer ondersteund?
- Duur: hoeveel tijd neemt een typische update/upgrade in beslag?
- Initiatief: gebeurt het onderhoud uitsluitend op initiatief van de kandidaat-leverancier of kan dit ook op initiatief van het ziekenhuis (bijv. wanneer het ziekenhuis een update om interne reden nog even wenst uit te stellen)?
- Uitvoering: wordt een update/upgrade door personeel van de kandidaat-leverancier uitgevoerd of door ziekenhuismedewerkers? Indien door ziekenhuismedewerkers: is er een stand-by support voorzien tijdens de procedure?
- Zijn bij elke upgrade de nodige software release notes voorhanden?

De kandidaat-leverancier dient tenslotte uitdrukkelijk te vermelden op welke manier hij met softwarebugs omgaat, d.i. op welke termijn die worden opgelost, welke garanties dienaangaande worden geboden, … .

2.3 Onderhoudscontract

Jan Yperman Ziekenhuis wenst voor de aangeboden oplossing een onderhoudscontract af te sluiten. Het onderhoudscontract moet deel uitmaken van de offerte.

Een onderverdeling rond onderhoud dient gemaakt te worden in volgende onderdelen:

- hardware koppelingen;
- softwarecomponenten – standaardpakket
- softwarecomponenten – maatwerk

Als onderdeel van het onderhoudscontract wenst Jan Yperman Ziekenhuis eveneens een verbintenis voor dagelijkse support. Het ziekenhuis ziet dit onder de vorm van een SLA-overeenkomst. Binnen deze overeenkomst wordt het plan van aanpak van de leverancier opgenomen, we denken hierbij aan telefoonnummers, Call-registratie, responstijden, opvolgingswijze, resultaatsverbintenissen enz. De inschrijver wordt geacht een voorstel van SLA als onderdeel van de offerte aan te bieden conform de in het lastenboek beschreven criteria.

2.4 Business Continuity

De leverancier vermeldt op welke manier er onderbrekingen (gepland en niet gepland) worden opgevangen zodat de algemene werking niet in gevaar komt. Dit zowel voor Cloud – Saas, als voor on premise toepassingen.

We denken hierbij bvb. aan het voorzien van een hot standby database, het regelmatig weggeschrijven van PDF’s op strategische plaatsen enz. en de werkwijze hoe die kan worden geraadpleegd bij problemen. Hierbij wordt tevens rekening gehouden met security policies.

3 DOCUMENTATIE EN OPLEIDINGEN

3.1 Architectuur

De kandidaat-leverancier dient de nodige architectuur documentatie aan te leveren, die de voorgestelde oplossing ondersteunt.

Architectuur documentatie kan bestaan uit:

- Applicatie Architectuur : blueprint van het applicatielandschap en de onderlinge interactie tussen de applicaties.
- Technologie Architectuur: de logische software en hardware mogelijkheden om de business, data, en applicatie services te draaien. Omvat de IT infrastructuur, middleware, networks, communicatie, processing, standards, etc.

3.2 Documentatie

Alle documentatie is Nederlandstalig of engelstalig en digitaal beschikbaar.

De leverancier zal naast de opleiding tevens alle nodige technische & operationele documentatie opleveren opdat de ICTmedewerkers van Jan Yperman Ziekenhuis het platform kunnen ondersteunen.

Er is een nederlandstalige gebruikershandleiding beschikbaar die via een helpfunctie geraadpleegd kan worden vanuit de toepassing.

Ook dient de inschrijver de nodige documentatie te voorzien over de opgeslagen data. Dit kan in de vorm van entity-relationship-diagram (ERD) van de gehele databank of een specifieke view met de nodige documentatie van de tabellen. Voor databases gehost buiten het Jan Yperman Ziekenhuis kan als alternatief een web API voorzien worden. Deze webservice moet voorzien zijn van de juiste documentatie. Aanpassingen aan de web API worden voor de wijziging meegedeeld. Eventuele alternatieven worden in detail beschreven. Dit is met name om beleidsondersteunende informatie te kunnen extraheren en te koppelen aan onze datawarehouse. Hiervoor is Jan Yperman Ziekenhuis bereid een non-disclosure formulier te ondertekenen. De documentatie wordt steeds up-to-date gehouden en bij wijzigingen ondersteund door de nodige documentatie binnen de release notes.

De klant kan na onderling overleg de toestemming krijgen om data rechtstreeks in de database te wijzigen of aan te vullen.

3.3 Opleidingen

De aanbieder zal kennisoverdracht en opleiding verzorgen aan de ICT medewerkers van Jan Yperman Ziekenhuis indien van toepassing. Deze opleidingen vinden plaats bij Jan Yperman Ziekenhuis.

Deze omvat:

- Algemene kennis overdracht sessies
- Kennis van de opbouw van de oplossing

- Technische kennisoverdracht en opleiding over de oplossing
- Kennis overdracht van operationele activiteiten, do’s, don’ts, en best practices.
- …