HELSE SØR-ØST

Prosjekt:

Nytt klinikk- og protonbygg Radiumhospitalet

Tittel:

Bilag D17

IKT-teknisk rammeverk og informasjonssikkerhet

02	For implementering	30.09.18	CHN	ENE	PMH
01	For intern tverrfaglig gjennomgang	14.08.18	CHN	ENE	ØYL
Rev.	Beskrivelse	Rev. Dato	Utarbeidet	Kontroll	Godkjent

Kontraktor/leverandørs logo:	Bygg nr:	Etasje nr.:	Systemgr.:	Antall sider:
				Side 1 av 15

Prosjekt:	Kontrakt nr:	Fag:	Dok.type:	Løpenr:	Rev.nr.:	Status:
RAD	**0000**	**Z**	**SP**	**0017**	**02**	**G**

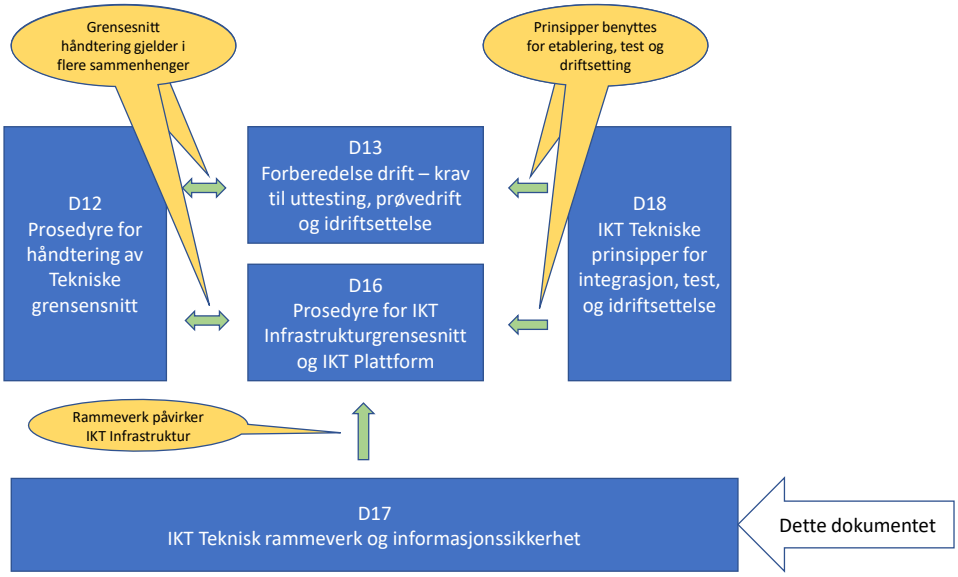
Innholdsfortegnelse

1 Innledning

Bilaget presenterer en sammenfatning av teknologistandarder og tilhørende krav og føringer som forutsettes benyttet ved leveranser til nytt Klinikk- og Protonbygg Radiumhospitalet (RAD).

1.1 Formål

Bilaget skal benyttes av Entreprenør/Leverandørene og valgt tilnærming skal avstemmes mellom Entreprenør/Leverandør og Byggherre for å sikre at teknologistandarder og tilhørende krav og føringer etableres slik at krav til forvaltning, drift, vedlikehold og informasjonssikkerhet ivaretas. Figuren nedenfor beskriver sammenhengen mellom omkringliggende bilag vha. gule merknader.



Figur 1 Sammenhengen mellom ulike bilag

Bilaget inngår i alle forespørsler som blir sendt ut for nytt Klinikk- og Protonbygg til Radiumhospitalet. På grunn av at teknologien er preget av hurtige endringer vil det kunne bli revidert jevnlig (typisk 1 gang per år). Dokumentet vil derfor være et dynamisk dokument.

IKT Infrastruktur (Kablingssystemet og datanettet) ved nytt Klinikk- og Protonbygg Radiumhospitalet er bærer av alle tjenester over IP på lokasjonen.

Andre utstyr- og teknologistandarder enn de som er nevnt i dokumentet kan ikke tas i bruk uten at det på forhånd er avklart og avtalt, ref. «Bilag D16 Prosedyre for håndtering av IKT Infrastruktur grensesnitt og IKT Plattform».

Dokumentet er utarbeidet med bakgrunn i de IKT-teknologi standardene som er i bruk i Helse Sør-Øst pr. august 2018, og som forventes å ville være gjeldende standarder ved oppstart av

Nytt Klinikk- og Protonbygg Radiumhospitalet i 2023. Det er forventet en utvikling i disse standardene frem til 2022.

Føringene i dette dokumentet gjelder alle løsninger som benytter felles IKT infrastruktur og IKT Plattform slik som Medisinsk Teknisk Utstyr (MTU), ByggTeknisk Utstyr (BTU), Administrativt Teknisk Utstyr (ATU), og IKT infrastruktur.

1.2 Målgruppe

Dokumentet er rettet mot Byggherren, Entreprenørene/Leverandørens løsningsansvarlige, IKT Infrastruktur koordinator (ref. Bilag D16), Helseforetakets tjenesteleverandør (Sykehuspartner HF) og Helseforetaket (OUS).

1.3 Begrep

I dette bilaget benyttes Helseforetaket som betegnelse for OUS. Innholdet i bilaget er utarbeidet av Helseforetaket sammen med Sykehuspartner som et generelt dokument som benyttes ved alle system og utstyrsanskaffelser.

Videre benyttes Leverandør som betegnelse på Totalentreprenør, Entreprenør eller Leverandør.

Forklaring til Forkortelser og øvrige begrep er gitt i kapittel 11

2 Føringer for Systemløsninger

Ved leveranser av systemløsninger skal Leverandøren fremlegge et overordnet løsningsdesign med systemdokumentasjon, som på en tydelig og oversiktlig måte viser de relevante hovedkomponenter, overordnet dataflyt og kommunikasjonsgrensesnitt internt og eksternt for løsningen. Dette gjelder uavhengig av om løsningen består av:

- For Medisinsk Teknisk Utstyr (MTU): Kun programvare, kun enkeltstående MTU eller sammensatte systemløsninger med server(e), MTU(er) og klient-PCer for MTU-styring/overvåking og datahøsting fra MTU.
- For byggnær IKT (BTU): Kun programvare, kun frittstående utstyrsenheter eller sammensatte tekniske anlegg/system med server(e) og klient-PCer for styring, regulering og overvåkning
- For administrativt teknisk utstyr (ATU): Kun programvare, frittstående utstyrsenheter eller sammensatte løsninger med server(e) og klient-PCer

Det er derfor meget viktig at dokumentasjonen gjenspeiler løsningen, uansett størrelse og omfang, eksempelvis med en tilhørende illustrasjon, slik den er tenkt etablert. Dokumentasjonen skal inkludere alle enkeltkomponenter i systemet (instrumenter, klient-PC, servere, lagring, nettverk, konvertere m.m.). Dette inkluderer også detaljert dataflyt mellom løsningens enkeltkomponenter, med eksisterende tjenesteelementer i Helseforetakets nettverk samt eventuelle behov for ekstern dataaksess.

Merknad: *Med «relevant» menes dataflyt som benytter eller traverserer datanettverk og derfor kan kreve at brannveggregler må tilrettelegges for at den tilbudte løsningen skal fungere i Helseforetakets IKT-infrastruktur.*

Hvis en løsning er basert på bruk av eksterne tjenester hos Entreprenør/Leverandør og/eller Produsent (skytjenester, web-portal eller tilsvarende), skal tilbudet også inneholde relevant løsningsdesign og Risiko og sårbarhetsanalyse (ROS) for leverandørens benyttede infrastruktur til produksjon av de nødvendige tjenestene som tilbudt løsning er avhengig av.

2.1 Overvåking og endrings-/oppdateringsregime

Sykehuspartner overvåker alle elementer som inngår i deres drifts- og forvaltningsregime. Leverandørløsninger og deres underliggende komponenter skal derfor tilby mekanismer og/eller grensesnitt for overvåking for å minimere forekomster av feil og nedetid.

For å sikre høyest mulig tjenestekvalitet er det en målsetning i Helseforetaket at det bare bør benyttes komponenter som har gyldige, produsentspesifikke vedlikeholdsavtaler gjennom hele kontraktsperioden. Helseforetaket har derfor preferanse for leverandører som i best mulig grad kan tilby en dokumentert og forpliktende roadmap for oppgradering og videreutvikling av sine løsninger.

I de tilfellene der en leverandør også skal ivareta drift- og forvaltningsoppgaver, så skal leverandøren både forholde seg til og etterleve det til enhver tids gjeldende endringsregime[1] for produksjonssatte løsninger.

2.2 Redundans

Helseforetaket skal ha mulighet for å bestille tjenester med høyest mulig oppetid på sine lokasjoner. Dette stiller krav til redundans helt opp på systemnivå. Med dette menes også redundans på eksempelvis server- og nettverksløsninger som inngår i tjenesten eller som tjenesten er avhengig av for å levere med avtalt tjenestekvalitet og/eller oppetid. Viktige elementer for å ivareta nødvendig redundans på tjenester er:

- En systemløsning bør ha mulighet for intern lastbalansering
- En systemløsning bør ha mulighet for ekstern lastbalansert nettverkstilkobling
- En systemløsning bør ha mulighet for intern redundans (failover)
- En systemløsning bør ha mulighet for redundant ekstern nettverkstilkobling (failover)

Et kompenserende tiltak for manglende redundans er evne til lokal overlevelse for en tjeneste ved bortfall av andre tjenester som eksempelvis nettverksforbindelse. En tjeneste må da kunne

[1] *Med endringsregime menes de reglene som gjelder for planlegging, varsling og utførelse av endringer på infrastruktur hos Helseforetaket og/eller Helseforetakets tjenesteleverandør, inklusive sentrale datasentre i Helse Sør-Øst. Dette omfatter all fysisk infrastruktur som strøm/kjøling, fysisk kabling, nettverk, nettverkstjenester, serverplattformer (fysiske og virtuelle) som den tilbudte løsningen er avhengig av for å kunne produsere de avtalte tjenestene. All endring som leverandør ønsker å utføre må være avtalt og omforent med Helseforetakets tjenesteleverandør da dennes arbeid alltid har forrang ved kollisjon på tidsluker. Dette for å unngå at planlagt vedlikehold kan feile under utføring med tilhørende driftsforstyrrelser og fare for pasientsikkerheten.*

mellomlagre resultater inntil nettverksforbindelse er operativ igjen og datasynkronisering kan gjennomføres.

3 Basis IKT Infrastruktur

3.1 Utstyrsmontasje

Entreprenørens utstyr skal plasseres i skap i ulike kommunikasjonsrom. Skapene vil være 80 x 100 x 240 cm i KR og 100 x 120 x 240 cm i HKR/SHKR Skapene vil bli utstyr med 19'' ramme. Utstyret kan enten rackmonteres eller plasseres på hyller. Skap vil bli utstyrt med 2 PDUer som er forsynt fra to ulike strømkurser (UPS).

For utstyr som skal plasseres utenfor kommunikasjonsrom må det særskilt angis behov for strøm (eventuelt UPS) og kjøling.

3.2 Kabling

Utstyr som inneholder intern kabling, skal grensesnitt mot både logisk og fysisk nettverk beskrives. Utstyr skal tilknyttes datanettet vha.:

- RJ45 Cat 6A/ea
- Fiber LC Single modus
- WLAN – 802.11a, g, n, ac el.

4 Nettverk

Helseforetaket har et nettverk som er klargjort for IPv6, men inntil videre benyttes kun IPv4. Fra Helseforetaket sin side, er løsninger som benytter tildelt IP-range (statisk eller DHCP) preferert.

Sykehuspartner er i dag Helseforetakets tjenesteleverandør av nettverksinfrastruktur med tilhørende nettverkskomponenter som svitsjer, rutere, brannmurer, fysisk kabling o.l. MTU/BTU/ATU-tjenester vil normalt etableres logisk adskilt fra andre tjenester og Helseforetakets administrative nett forøvrig. Ved behov åpnes det for tilgang mot annet MTU og integrasjoner mot andre tjenester i Helseforetakets nettverk, som f.eks. fagsystemer.

Helseforetaket er pålagt å ha høyt fokus på Informasjonssikkerhet. Helseforetaket har derfor bygget opp en omfattende nettverkssegmentering og soneinndeling for å ivareta behov for trafikksegregering og etablering av sikkerhetsregimer. Eksempelvis benyttes Network Access Control (802.1x) som stenger ned LAN-tilgang og VLAN-tilhørighet for ukjente eller inaktive enheter. I utgangspunktet tillates det ikke at utstyr (servere, PC, devicer etc.) kan settes opp som mulige gateway-maskiner (dvs. skal ikke ha to eller flere nettverkskort) mellom ***et internt nett og Helseforetakets sitt datanettverk***. I slike tilfeller skal tjenesten inkludere en godkjent ruter/brannmur som **separerer** løsningen fra Helseforetaket sitt datanettverk.

Det benyttes i tillegg standardisert brannmursregulering mellom nettverkssoner hvor inaktive TCP-sesjoner termineres av sikkerhetsgrunner etter 60 eller 120 minutter. Dette legger krav på det utstyret som skal kobles opp i nettverket, og Leverandør må ta hensyn til dette i sine løsninger.

All bruk av konvertering mellom Ethernet og andre interfaceteknologier må dokumenteres detaljert for å sikre at de tilbudte løsningene er teknologikompatible og kan benyttes i et kundespesifikt design. Helseforetaket ønsker at all form for trådløs kommunikasjon skal benytte standard teknologier og protokoller som WLAN, Bluetooth, GSM/LTE, annen RF.

5 Maskinvare

Sykehuspartner er i dag Helseforetakets tjenesteleverandør av maskinvare som klient-PCer, servere (fysiske og virtuelle), lagringsløsninger, skrivere, skannere og strekkodelesere med mere. Hvis tjenester ikke skal etableres på leverandørspesifikt utstyr, må alle HW/SW-relaterte behov fra leverandørens side være formidlet til Sykehuspartner.

Merknad: *Eksempel: RAM, CPU, OS (HOST/GUEST), disk, RAID, tilkoblingskort, lagringsprinsipper, filsystem, diskvolum, lese/skrivehastighet o.l.*

Helseforetaket har standardisert på bruk av «Pull Print» (sikker print). Det er derfor viktig at integrasjon mot en slik printløsning er mulig hvis en tjeneste behøver utskrift. Dette vil normalt krever integrasjon mot, alternativt innmeldes i, Helseforetakets AD for nødvendig brukerhåndtering.

6 Operativsystem og programvare

I dag er standard operativsystem Windows 10 på klient-Pcer og Windows Server 2016 I tillegg supporterer Tjenesteleverandør nyere versjoner av RedHat Linux.

Gjennom Tjenesteleverandørens avtaleverk er målsetningen at alle løsninger skal støtte en såkalt «N/(N-1)»-livssyklus for alle de systemkomponenter som inngår i en løsning. Dette betyr at det skal benyttes siste, eller nest siste, versjon av alle HW/SW-komponenter som inngår i leveranser gitt gjennom Sykehuspartner der de drifter komponentene som inngår i en levert tjeneste.

Gjeldene standard software for anti-malware er i dag Trend på Windows servere og Microsoft System Center Endpoint Protection (SCEP) på Windows-klienter. For databaser er gjeldende standard Microsoft SQL Server 2014 og Oracle Enterprise R12.

I de tilfeller hvor Leverandør står ansvarlig for utstyrsleveranser, inklusiv OS, skal det gjennomføres relevant «herding» av OS og benyttede applikasjoner på det Leverandørspesifikke utstyret.

Det benyttes RES One Suite fra RES (res.com) for styring og sikring av klientarbeidsflater, inkludert tilgjengeliggjøring av klientapplikasjoner med alle tilhørende plugins og 3.partskomponenter. Distribusjon av applikasjoner gjøres hovedsakelig via APP-V, alternativt via SCCM.

6.1 Behov for Systemkomponenter

Hvis leverandørens tjeneste krever spesielle systemkomponenter for at den tilbudte løsningen skal fungere som avtalt, så må dette avtales og tilgjengeliggjøres gjennom Helseforetaket og Sykehuspartner. Slike systemkomponenter bør kunne hentes fra gjeldende produkt- og

tjenestekatalog fra Sykehuspartner. Eksempelvis kan Sykehuspartner utstede nødvendige sertifikater til bruk for HTTPS/SSL i serversammenheng etter nærmere avtale. Eksempler på slike systemkomponenter kan være nettleser, webserver[2], databaser, Java, Flash, Silverlight, MS Office, .NET Framework, C++ Redistributable, MDAC o.l. og eventuelle spesifikke versjoner av disse.

Tjenester fra eksterne leverandører bør ikke til enhver tid være avhengig av kommunikasjon med webtjenester utenfor Helseforetakets nettverk, eksempelvis hos Leverandør/Produsent eller direkte mot internett.

Merknad: *Helseforetaket krever kontroll og sporbarhet på all ekstern kommunikasjon. Godkjent dokumentasjon på hvorfor slik kommunikasjon er påkrevd, og i hvilken grad løsningen ivaretar Helseforetaket sine sikkerhetskrav til ekstern kommunikasjon må derfor alltid eksistere.* Endelig bruk av slik kommunikasjon krever en gjennomført risikovurdering som gir en godkjenning.

6.2 Sikkerhetsformalia

Av hensyn til informasjonssikkerhetskrav bør en tjeneste benytte kryptering på applikasjonsnivå ved datautveksling med andre systemer.

Bruk og/eller vedlikehold av installert programvare på servere og klienter (utover selve OS-installasjonen) på server bør skje uten bruk av lokal administratorrettighet på operativsystemet.

I de tilfeller der servere og klienter ikke leveres gjennom Sykehuspartner har Helseforetaket følgende sikkerhetsprinsipper:

- Servere og klienter som inngår i den tilbudte løsningen bør ha mulighet for å meldes inn i Helseforetaket sitt AD
  AD-innmeldte klient-Pcer som skal benyttes i den tilbudte løsningen bør benytte diskkryptering (eks. MS BitLocker).
- Sikkerhetspatcher og servicepacks bør kunne installeres automatisk, enten unmanaged eller ved neste omstart av klient eller server
- Klientapplikasjon(er) bør være kompatibel med bruk av RES One og App-V samt SCCM.

7 Informasjonssikkerhet og tilgangsstyring

Helseforetaket stiller strenge krav til Informasjonssikkerhet i forbindelse med etablering og drift av MTU/BTU/ATU-løsninger. MTU/BTU/ATU skal beskyttes mot eksterne trusler, sykehusnettet og annet MTU/BTU/ATU. Sykehusnettet skal på sin side beskyttes mot MTU/BTU/ATU.

Helseforetaket plikter å oppfylle lovreglene i personvernforordningen (GDPR). Det stilles derfor krav til at tilbudt løsning skal tilfredsstille krav i Personvernforordningen artikkel 25 – Innebygd personvern, se:

---

[2] *Hvis tilbudt løsning benytter lokal webserver bør det være implementert mekanismer som sikrer server og innhold mot uautorisert tilgang. Det skal i så fall være dokumentert hvilke sikkerhetsmekanismer som er aktivert, samt hvilke mekanismer som kan aktiveres i tillegg.*

- Datatilsynets veileder for innebygd personvern – https://www.datatilsynet.no/regelverk-og-verktoy/veiledere/programvareutvikling-med-innebygd-personvern/
- Datatilsynets informasjon om personvernforordningens krav til innebygd personvern til leverandører og utviklere i helse- og omsorgssektoren – https://www.datatilsynet.no/personvern-pa-ulike-omrader/forskning-helse-og-velferd/leverandorer-og-utviklere-i-helse–og-omsorgssektoren/
- GDPR – Article 25, Data protection by design and by default (på Engelsk) – http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL

Helseforetaket er pålagt å etterleve Direktoratet for eHelse sin «Norm for informasjonssikkerhet» («Normen»), se:

- «Normen» - https://ehelse.no/personvern-og-informasjonssikkerhet/norm-for-informasjonssikkerhet
- Veileder i personvern og informasjonssikkerhet – medisinsk utstyr – https://ehelse.no/personvern-og-informasjonssikkerhet/norm-for-informasjonssikkerhet/normen/veileder-i-personvern-og-informasjonssikkerhet-medisinsk-utstyr
- «Normen» (på Engelsk) – https://ehelse.no/personvern-og-informasjonssikkerhet/norm-for-informasjonssikkerhet/documents-in-english

Eksempler på føringer gitt av personvernforordningens krav til innebygd personvern og «Normen» er:

- Helseforetaket prefererer løsninger der det benyttes individuell brukeridenter med sikret rollebasert tilgangsstyring
- Løsninger skal ikke lagre personopplysninger som navn, fødselsnummer, rekvisisjonsnummer, diagnose, prøveresultat og lignende på permanent basis uten at krav til Informasjonssikkerhet er ivaretatt
- Helseforetaket har som målsetning å standardisere integrasjonstjenesten på Helse Sør-Øst sin Regionale Integrasjonsplattform for alle former for integrasjon mellom nettverks- og sikkerhetssoner. Dette gjelder både socket-basert kommunikasjon og filflytt.
- For løsninger som krever bruk av eksternt lagringsmedium for manuell overføring av datafiler retter Helseforetaket seg etter retningslinjene fra regionalt styringssystem for informasjonssikkerhet, ref. http://ehandboken.ous-hf.no/document/109656, punkt 4.3: «Kryptering under lagring av data»[3].

Hos Helseforetaket har man derfor gjeldende relevante føringer for å ivareta krav til informasjonssikkerhet:

- Løsninger bør benytte sentralisert fillagring og/eller database

3 I dag benyttes krypterte lagringsenheter fra IronKey hos Helseforetaket

Løsninger bør benytte individuelle brukeridenter både på OS- og applikasjonsnivå, og individuell LDAP-brukerautentisering bør gjøres mot grupper definert i Active Directory.

- Alle former for lokale brukerprofiler (brukernavn/passord) lagret i lokale brukerdatabaser, konfigurasjonsfiler e.l. som benyttes til klient-, database- eller applikasjonspålogging bør sikres med standardiserte mekanismer for tilgangskontroll og kryptering.
- Løsninger bør støtte rollebasert og eller beslutningsstyrt tilgangsstyring.
- Løsninger bør ha funksjonalitet for begrensning av tilgang til personopplysninger for enkeltbrukere og grupper av brukere
- Hvis løsninger inneholder standard- eller systembrukere, så bør det bare benyttes unike passord før tilkobling til Helseforetakets IKT-infrastruktur
- Det skal ikke benyttes passord som kan hentes direkte fra brukermanualer eller annen form for tilgjengelig dokumentasjon
- Helseforetaket har strenge føringer til logging og sporbarhet av bruker- og systemaktivitet. All slik logging må møte gjeldende føringer for Informasjonssikkerhet knyttet til Integritet, Konfidensialitet og Tilgjengelighet.
- Ved eventuelt behov for ekstern lagring eller manuell videreformidling av person- eller pasientsensitiv data, er det en sentral føring at slike løsninger benytter krypterte USB-lagringsenheter fra IronKey
- Hvis løsninger benytter eksterne webløsninger/-portaler for analyse, rapportering eller drift og forvaltning bør løsningen oppnå en «Overall Rating» på rapport generert hos Qualys SSL Labs4 på minst «A»
- Løsningen bør ha funksjonalitet for automatisert sletting av personopplysninger, når disse er prosessert eller bekreftet overført til fagsystem.

8 Backup

Helseforetaket ønsker å etterleve prinsippene om Data Lifecycle Management hvor Backup/Restore er en sentral komponent for å ivareta datasikkerhet og integritet. Målsetningen er at leverandørtjenester kan benytte eksisterende tjeneste fra Sykehuspartner for sentralisert Backup/Restore i størst mulig grad. Dette vil gjelde for både server, klient og databaser.

Det forutsettes at nødvendige backupklienter kan installeres i den aktuelle løsningen og eventuelle leverandørspesifikke brannmurer åpnes for tilgang fra backupløsning.

Databaser som inngår i den tilbudte løsningen bør ha støtte for både full og inkrementell backup (gjennom f.eks. loggbackup/loggshipping) av databaser.

4 Qualys SSL Server Test er en åpen verifisering av kryptering. https://www.ssllabs.com/

9 Integrasjoner

Hvis den tilbudte løsningen benytter datautveksling med sentrale kundesystemer, bør dette skje med bruk av åpne eller de Facto standarder for slik datautveksling. Spesielt viktig er integrasjoner mot sentralsystemer som DIPS, Metavision, UniLab/SwissLab mm.

Helse Sør-Øst har en Regional Integrasjonsplattform for all integrasjon og samhandling internt i helseforetaket, mellom helseforetak og med eksterne aktører. Denne plattformen inneholder standardiserte integrasjonstjenester, basert på internasjonale og nasjonale meldingsstandarder. Eksempler på slike standarder er HL7, FHIR, KITH og DICOM (DICOM er standard for MTU-kommunikasjon mot RIS / PACS). Eksempler på kjente og benyttede kommunikasjonsprotokoller er http(S), FTP, SFTP/FTPS, CIFS.

Ved systemløsninger der det er integrasjonsbehov (overføring av data til sentrale systemer) er det derfor meget viktig at løsningene støtter den Regional Integrasjonsplattformen som er etablert i Helse Sør-Øst. Dette gjelder viktige elementer som loggfunksjonalitet, sikkerhetsmekanismer, benyttede kommunikasjonsprotokoller, meldingsformater og semantikk. Alle disse faktorene vil påvirke tidsforbruk og kostnad ved en etablering av integrasjon.

Viktige elementer som skal hensyntas i slike situasjoner er:

- I hvilken grad inkluderes API eller tekniske løsninger for å tilpasses en Integrasjonsløsning, eksempelvis: Webservice, fileksport/import, WCF, DICOM
- Benyttes API på en sikker måte for integrasjon og informasjonsutveksling
- Gjøres utveksling av medisinsk informasjon (HL7, FIHR, KITH, DICOM, ASTM eller lignende) uten leverandørspesifikke krav eller begrensninger i forhold til hvilke protokoller som kan benyttes, eksempelvis: TCP/UDP, FTP/FTPS/SFTP, CIFS, SMTP, SOhttpHTTP/HTTPS), MSMQ, DICOM.
- Kan integrasjon og informasjonsutveksling gjøres uten at det stilles leverandørspesifikke krav eller begrensninger til hvilke meldingsformater som kan benyttes, eksempelvis: XML, CSV, DICOM
- Kan det gjøres logging av meldingsflyt og meldingskvitteringer ved bruk av integrasjonstjenester, *samt hvilken loggfunksjonalitet som eksisterer for å understøtte behov for meldingsdokumentasjon, eventuell feilsøking og analysering av avvik på sendte og mottatte data*

10 IKT-Relatert drift og forvaltning

Helse Sør-Øst har standardisert metodikken for eksterne leverandørers fjernaksess gjennom løsninger fra F5 BigIP og Citrix. Helseforetaket tilbyr i dag en standard fjernaksessløsning for alle eksterne utstyrsleverandører. Den benevnes «Leverandøraksess» og skal benyttes for all leverandørspesifikk drift og forvaltning der det ikke forutsettes personlig oppmøte i Helseforetakets lokaler. For å kunne bruke denne løsningen må Leverandør kunne benytte web-plugin for SSL VPN og Citrix Receiver web-klient på sine PC-er. Leverandøren får da tilgang til en

aksesserver hos Helseforetaket, hvor nødvendig programvare og/eller fjernstyringsprogram mot MTU-klient/-server gjøres tilgjengelig. All bruk av fjernaksessløsningen skal knyttes til personlige, identifiserte brukere hos Leverandøren.

Det er videre en standardisert «filsluse» for kontrollert og sikker overføring av godkjente data mellom Helseforetaket og Leverandør.

Det er etablert en regional VPN-Gateway for terminering av VPN-forbindelser mellom Leverandører og Helseforetaket. Dette er den foretrukne metoden for utgående datatransport over VPN fra Helseforetaket sitt nettverk når tilbudt løsning via filsluse ikke gir tilstrekkelig funksjonalitet. All planlagt bruk av slik dataoverføring over VPN må først risikovurderes og godkjennes før dette kan etableres. Leverandøren skal ved en slik godkjenningsprosess gi en forpliktende forsikring/dokumentasjon på benyttede dataformater, at VPN-bruken kun omfatter tekniske data, og at det ikke er risiko for overføring av personopplysninger, inkludert krypterte. Alle ønskede endringer i formatoppsett og bruk av VPN skal godkjennes av Helseforetaket i forkant før endringer kan gjennomføres.

Det er sentralt og viktig for både Helseforetaket og Sykehuspartner at utstyr i nettverket kan tilby loggingsfunksjonalitet på flere nivåer som hardware, OS, sikkerhet, brukeraktivitet med mere. Alle logger som den tilbudte løsningen genererer der innholdet må klassifiseres som virksomhets- eller personsensitivt, må sikres i henhold krav om informasjonssikkerhet (ref. «Normen»). Dette må gjøres for å sikre at essensiell logginformasjon ikke kan leses, endres eller slettes av uautorisert personell.

Hvis Helseforetaket er omforent med Leverandør om at drift og forvaltning krever bruk av Leverandøraksess, så må det som hovedregel inngås databehandleravtale med Sykehuspartner. I dag gir Leverandøraksess tilgang til aksesserver med forhåndsinstallerte forvaltnings- og driftsverktøy som UltraVNC, WinSCP, RDP og SSH. Bruk av egendefinert intern leverandøraksess med løsninger som 3G/4G-eller ADSL-modem, samt programvare som TeamViewer, LogMeIn etc. tillates ikke av Helseforetaket[5].

11 Forkortelser og begreper

Begreper	Beskrivelse
3G/4G-modem	USB-modem benyttet til 3G/4G GSM-kommunikasjon
AD	Active Directory – Microsofts katalogtjeneste for autentisering og autorisering av brukere innenfor et Windows domene
ADSL	Asymmetric Digital Subscriber Line - linje for dataoverføring via kobberkabel/telefoninett
API	Application Programming Interface, grensesnitt for integrasjon
ASTM	Standardiseringsorgan for internasjonale standarder, bl.a. innenfor labkommunikasjon.
Bluetooth	Teknologi for trådløs kommunikasjon
Byggherre	Ivaretar Helseforetakets rolle i forholdet til entreprenør/leverandør i forbindelse med gjennomføring av byggeprosjektet

[5] *Hvis en Leverandør har behov for å få tilgjengeliggjort annen programvare i Helseforetaket sin standard fjernaksessløsning må det søkes om og godkjennes.*

Begreper	Beskrivelse
CIFS	Common Internet File–System - protokoll for fil-share
CSV	CSV - Comma Separate– Values - tekstfil inneholdende data separert med komma eller annet tegn for separasjon av felt
DICOM	Digital Imaging and Communications in Medicine – standard for utveksling av bildefiler
DNS	Domain Name System - Systemtjeneste for å oversette mellom maskinnavn og IP-adresse
ebXML	Electronic Business using eXtensible Markup language - XML standarder for bruk ved elektronisk overføring av forretningsinformasjon
Ekstern datautveksling	Med ekstern datautveksling menes all datatrafikk som benytter Helseforetakets infrastruktur. Dette kan eksempelvis være kommunikasjon med sentraliserte tjenester for autentisering og autorisering av brukere, fillagring, database, eller integrasjon med andre tjenester.
Endringsregime	Med endringsregime menes de reglene som gjelder for planlegging, varsling og utførelse av endringer på Helseforetakets infrastruktur, inklusive sentrale datasentre i Helse Sør-Øst. Dette omfatter all fysisk infrastruktur som strøm/kjøling, fysisk kabling, nettverk, nettverkstjenester, serverplattformer (fysiske og virtuelle) som den tilbudte løsningen er avhengig av for å kunne produsere de avtalte tjenestene. All endring som leverandør ønsker å utføre må være avtalt og omforent med Sykehuspartner da dennes arbeid alltid har forrang ved kollisjon på tidsluker. Dette for å unngå at planlagt vedlikehold kan feile under utføring med tilhørende driftsforstyrrelser og fare for pasientsikkerheten.
EPJ	Elektronisk pasientjournal
Fagsystem	System som ivaretar særskilte funksjoner innen ett eller flere fagfelt. Eksempelvis LIMS eller EPJ
F5 BigIP VPN	Standard leverandøraksess via VPN leveres gjennom produktet BigIP fra F5
FHIR	Fast Healthcare Interoperability Resources –er en standard som beskriver dataformater og elementer og et programmeringsgrensesnitt (API) for utveksling av informasjon knyttet til elektroniske helsejournaler. Standarden ble opprettet av Health Level Seven International (HL7).
Firewire	IEEE1394, teknologi for kablet høyhastighets dataoverføring
FTP/FTPS	File Transfer Protocol/File Transfer Protocol m/SSL-kryptering, protokoller for filoverføring
GDPR	General Data Protection Regulation (EU) 2016/679, EUs personvernforordning
GSM	Global System for Mobile Communications - standard for telekommunikasjon for mobiler
Helseforetaket	I dette dokumentet benyttes dette som begrep for de(t) aktuelle helseforetak(ene). Spesifikt for nytt klinikk- og protonbygg for Radiumhospitalet er dette OUS.
Herding	Herding av klient PC, server o.a. IKT-komponenter er en metode som benyttes for å øke komponentens sikkerhet ved å fjerne og begrense mulige sikkerhetsmessige sårbarheter som kan utnyttes av en angriper. Dette kan eksempelvis gjøres gjennom å sikre at operativsystem, programvare og 3.programvarekomponenter er sikkerhetspatchet eller oppdatert til siste versjon, bruk av antivirus/anti-malware, bruk av lokal brannmur, samt stoppe/sperre tjenester som ikke benyttes.
HL7	Health Level 7 – standard for meldingsutveksling av klinisk og administrativ informasjon mellom helserelaterte informasjonssystemer
HOST	Windows hosts fil, statisk tekstfil med oversikt over maskinnavn og korresponderende IP-adresse
HTTP/ HTTPS	HyperText Transfer Protocol/HyperText Transfer Protocol Secure - standarder for kommunikasjon for World Wide Web
IEEE 802.1x	Standard for autentisering av maskinvare tilkoblet nettverk. Må ikke forveksles med standarder for trådløst nett (WLAN).
IP-multicast	IP-kommunikasjon hvor data sendes samtidig til en spesifisert gruppe lyttende mottakere i nettverket

Begreper	Beskrivelse
IPv4	Standard adresseringsprotokoll for forbindelsesfri kommunikasjon i nettverk
IPv6	Siste versjon av IP-kommunikasjonsprotokoll som på sikt vil erstatte IPv4
Ironkey	Godkjent USB-lagringsenhet med krypteringsteknologi (www.ironkey.com)
KITH	Standard for meldingsutveksling av klinisk og administrativ informasjon mellom helserelaterte informasjonssystemer
Lagrings-løsning	Samlebegrep for ulike nettverkstilkoblede løsninger der data kan lagres eksternt. Eksempler er filserver (fysisk/virtuell), NAS/SAN
LAN	Local Area Network, kablet nettverk
LDAP	Lightweight Directory Access Protocol – Standard protokoll for tilkobling/integrasjon mot Active Directory
Leverandør	I dette dokumentet benyttes dette som begrep for den som leverer tilbud på bakgrunn av en anbudsforespørsel fra Helseforetaket
LIMS	Laboratory Information Management System, laboratoriesystem
MAC-adresse	Unik ID tildelt nettverksgrensesnitt på lag2 i OSI-modellen
MDD	Medical Device Directive
MS SCEP	Microsoft System Center Endpoint Protection – standard antivirusløsning for klient-PCer i HSØ
MSMQ	Microsoft Message Queuing – Microsofts løsning for meldingskø, støttet i de fleste versjoner av Windows
MTU	Medisinskteknisk utstyr
NAC	Network Access Control – Se IEEE 802.1x
NAS	Network Attached Storage
NAT/PAT	Network Address Translation/Port Address Translation – en metode for å mappe en IP-adresse/Port-range til en annen
OS	Operativsystem
OUS	Oslo Universitetssykehus HF
PACS	Picture Archiving and Communication System
Personopplysning	Enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»); en identifiserbar, fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator, f.eks. et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en online-identifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet
RAM	Internminne
RDP	Remote Desktop Protocol – Microsoft protokoll for fjernstyring av Windows PC/server
RF	Radiofrekvens
RJ45	Modulærkontakt benyttet for terminering av nettverkskabel (Ethernet)
Risikovurdering	Risikovurdering utføres ved nyetablering av, samt endringer på, eksisterende MTU-løsninger i HSØ. Risikovurderingen skal identifisere risiko og sårbarhet i løsningen, samt evt. risikoreduserende tiltak med ansvarlig for utførelse.
RS232	Seriellport – grensesnitt for seriell dataoverføring
SAN	Storage Area Network

Begreper	Beskrivelse
Sensitive personopplysninger	Se Særlige kategorier av personopplysninger
SFTP	FTP over SSH
SNMP trap	Simple Network Management Protocol, Trap – en metode for en klient å informere en overvåkningstjeneste om hendelser, som feil, i nettverk eller programvare.
SOAP	Simple Object Access Protocol - Protokoll for utveksling av strukturert informasjon over web-servicer vha. XML
SSH	Secure Shell - Applikasjonsprotokoll med kryptert kommunikasjon for tilgang til pålogging og kommandolinje på fjernstyrt klient/server
SSL	Secure Sockets Layer – Sertifikatbasert krypteringsprotokoll typisk benyttet for web
STP	Shielded Twister Pair, nettverkskabel med skjerming og mulighet for jording
Sykehuspartner HF	Helseforetakets Tjenesteleverandør. I tillegg vil Sykehuspartner ha ansvar for egne leveranser til byggeprosjektet (Nettverk og IKT utstyr)
Særlige kategorier av personopplysninger	Med særlige kategorier av personopplysninger (tidligere benevnt sensitive personopplysninger) menes i denne sammenheng: • Opplysninger regulert av Personvernforordningen artikkel 9 • Helseopplysninger som inneholder navn, fødselsnummer eller andre personentydige kjennetegn slik at opplysningene kan spores tilbake til en enkeltperson • Helseopplysninger der navn, fødselsnummer og andre personentydige kjennetegn er fjernet og erstattet med et løpenummer, en kode, fiktive navn eller lignende, som viser til en atskilt liste med de direkte personopplysningene, eksempelvis et rekvisisjonsnummer, prøve-ID e.l.
TCP	Transmission Control Protocol – Sikker kommunikasjonsprotokoll for applikasjoner som kommuniserer over et IP-nettverk
Tjeneste-leverandør	Det til enhver tid gjeldende selskap/organisasjon som har ansvar for drift- og forvaltningsansvar for Helseforetaket sin samlede IKT-infrastruktur og IKT-tjenestekatalog. Pt. er dette Sykehuspartner HF (SP)
UDP	User Datagram Protocol – Usikker kommunikasjonsprotokoll for applikasjoner som kommuniserer over et IP-nettverk
UltraVNC	Applikasjon for fjernstyring av klient/server gjennom fjernaksessløsning
USB	Universal Serial Bus – grensesnitt for tilkobling av periferiutstyr
VLAN	Virtual LAN - en måte for logisk inndeling av nettverk i separate broadcastdomener
VRF	Virtual Routing and Forwarding. En virtualiseringsteknologi som gjør det mulig å ha flere uavhengige rutingstabeller i en og ruter. Dette gjør det mulig å ha overlappende, eller identisk adresserom i rutingstabellene uten at det gir adressekonflikter. Man slipper da å etablere separate nettverk med flere fysiske rutere, alt kan etableres og segmenteres på en og samme ruter.
WCF	Windows Communications Foundation – Microsoft API for integrasjonstjenester
WINS	Windows Internet Name Service. Tjeneste definert av Microsoft for å mappe maskinnavn opp mot IP-adresse og tjenestetype maskinen kan tilby
WLAN	Wireless Local Area Network, trådløst nettverk
XML	eXtensible Markup Language - Standard for strukturerte data i tekstformat