ID	Beskrivelse av krav
	Funksjonelle krav
F1	Beskriv tilbudt løsning for EKG-database
F2	Det ønskes en integrasjon mellom EKG-databasen og sykehusets pasientjournalsystem DIPS. Tilbudt funksjonalitet for dette skal beskrives.
F3	Det skal være mulig å lagre EKG-kurver med tilhørende standard analyse som overføres fra EKG-apparatet.
F4	EKG-undersøkelsen må lagres i et format som gjør det mulig å utføre av målinger i etterkant.
F5	EKG-undersøkelser skal kunne tolkes (automatisk og manuelt) fra analyseprogrammet.
F6	Det skal være mulig å sammenligne tidligere undersøkelser med nye eller eldre resultater på samme pasient.
F7	Det bør være mulig å lagre tilhørende kliniske data ved EKG-undersøkelsen (eks.BP, Puls, WATT) og genererte rapporter (pdf).
F8	Det skal være mulig å lagre utvalgte sekvenser fra EKGet. Beskriv metode og format.
F9	Det skal være mulig å ta ut EKG-undersøkelser anynomisert til undervisning og forskning.
F10	Beskriv mulighet for forhåndsinnstilte skjermbilder/-oppsett.
F11	Ved å velge ett EKG i DIPS skal kun dette vises. Andre EKGer lagret på den aktuelle pasienten skal gjøres tilgjengelig.
F12	Det skal være mulig å søke og sortere på de ulike EKG-undersøkelsene i databasen eks. 12-avledet, stress-test, pre-hospital etc. Det skal også være mulig å søke og sortere på dato og avdeling.
F13	En EKG-undersøkelse bør ha informasjon om hvilket utsyr som ble brukt under undersøkelsen.

F14	Stress-EKG skal lagres som ett EKG, ikke flere forskjellige.
F15	Det bør finnes en funksjon for import av ergospirometritester.
F16	Det må være mulig å korrigere databasen når EKG er koblet til feil pasient.
F17	Applikasjonen må kunne startes alene, ikke kun gjennom DIPS
F18	Redgjør for mulighet for å starte DIPS gjennom applikasjonen.
F19	Undersøkelser som mangler delvis pasientinformasjon, bør legges i en egen katalog for verifisering mot DIPS. Beskriv løsning.
F20	Beskriv hvordan pasient-ID som er lagt inn på diverse EKG-utstyr, manuelt eller ved barcodescanner, overføres til EKG-databasen og verifiseres med DIPS.
F21	Et EKG opptak skal ikke bli lagret i databasen to ganger. Beskriv hvordan dette løses.
F22	Brukeren skal selv kunne redigere lengden på opptaket.
F23	Det skal være mulig å søke og sortere på de ulike EKG-enhetene i databasen, eks. 12-avledet, stress-test, pre-hospital, dato, avdeling etc.
F24	Hvor lang tid vil det ta å hente opp og vise EKG-undersøkelser fra EPJ?
F25	Kommunikasjonen fra EKG-utstyret til databasen og EKG-klientene skal være synkront (nettverkskontakt må være tilstede).
F26	Det bør sendes en bekreftelse til opptaksutstyret når EKGet er lagret i EKG databasen.
F27	Beskriv mulighet for automatisk sletting av EKG-opptaket fra utstyret ved bekreftelse fra databasen om at dataene er lagret.
F28	Beskriv mulighet for å vise EKG-undersøkelser på mobile enheter f.eks. tablet, mobil etc.
	Pasientinformasjon
F29	Følgende pasientdemografiske data skal vises for hver pasient: Navn, Pasient-ID, alder, kjønn.
F30	Redegjør for annen pasientinformasjon som kan hentes og lagres.
F31	Det skal være mulig å legge inn og lagre pasientens høyde og vekt.

F32	Man bør kunne legge inn pasient-ID på en lagret undersøkelse i systemet
F33	Rapport fra pre-hospitale enheter skal kunne overføres til EKG-databasen
F34	Det bør være mulig å overføre Holter-rapporter til databasen
F35	Det bør være mulig å overføre Holter-undersøkelser til databasen
F36	Det bør være mulig å gjennomføre en Holter-analyse i analyseprogrammet
F37	Det bør være mulig å importere standard filformater som XML, BMP, JPEG og konvertere dem til PDF
F38	Mulighet for automatisk oppdatering av pasientens demografiske data fra DIPS (eks. dødsfall, navne bytte, nytt personnummer) beskrives
	Analyseverktøy
F39	Tilbyder skal gi en beskrivelse av analyseverktøyet.
F40	Det skal være mulig å se forandringer fra tidligere EKG og innen det samme EKGet (Stress test). Følgende funksjoner skal være med: Frekvens, PQ-interval , QRS-tid, QT/QTc interval, P akse, QRS-akse, ST-segment deviation, Hypertrophy-kriterie
	Måleverktøy
F41	Gi en kort innføring/ beskrivelse av måleverktøyet
F42	Følgende måleverktøy bør være tilgjengelig: Intervall, A til B Intervaller. Horisontalt/ vertikalt, Parallelle intervaller, Mulig å bevege/ stille inn linjaler, Copy/paste linjal,Mulighet for å se på flere undersøkelser samtidig,Mulig å forandre på tidsoppløsningen. 25, 50, 100 mm/sek og dynamisk
	Automatiske målinger
F43	Automatiske målinger som blir gjort i arbeidstasjonene/applikasjonen, skal kunne manuelt korrigeres i etterkant og lagres i databasen. Følgende parametere bør inngå i den automatiske analysen: Rytme/frekvens, PQ-interval, QRS-tid, QT/QTc intevall, P-akse, QRS-akse, ST-segment deviation, Hypertrophy-kriteria
	Generelle dokumentasjonkrav
F44	Tilbyder skal utarbeide en framdriftsplan/gjennomføringsplan for installering og igangkjøring av løsningen.

F45	Tilbyder skal utarbeide forslag til designdokument og systemdokumentasjon.
	Medisinsktekniske krav
F46	Prouktet skal tilfredsstille de til enhver tid gjeldende standardkrav når det gjelder tiltenkt bruk (intended use)
F47	Tilbyder skal gi en oversikt over de internasjonale standarder produktet er produsert i henhold til.
F48	Produktet skal være CE-merket, både individuelt og i system, i henhold til det direktiv som gjelder for produktet.
	Krav til opplæring
F49	Tilbudet skal være inkludert brukeropplæring. Opplæringen skal skje på brukerstedet ved leveranse og som oppfølging etter avtale. I tilbudet skal omfang av og innhold i opplæringen beskrives.
F50	Det er ønskelig at opplæring foregår på norsk(skandinavisk)
F51	Ved levering/innstallasjon skal leverandøren gi en gjennomgang av det installerte systemet med hensyn på drift og vedlikehold
	Dokumentasjon
F52	Dokumentasjon inngår som en del av leveransen og skal være sluttlevert før godkjenning av leveransen.
F53	Komplett dokumentasjon skal fortrinnsvis leveres på norsk i elektronisk versjon og i papirversjon. For enkelte systemer kan det etter avtale leveres engelskspråklig manual.
F54	Det skal leveres brukermanual for systemet. Brukermanualen skal fortrinnsvis være på norsk og leveres både i elektronisk versjon og papirversjon.
F55	Det skal leveres en komplett funksjons- og vedlikeholdsbeskrivelsen av systemet (Driftsdokumentasjon).

ID	Beskrivelse av krav
	Krav til drift og vedlikehold
V1	Tilbyder skal ha en organisasjon med nødvendig relevant kompetanse. Beskriv organisasjonens oppbygning, lokasjon og kompetanse.
V2	Det vil bli vektlagt at Tilbyder har rask responstid ved akutte feil. Oppgi maksimal responstid (ikke normal responstid) fra feilmelding til oppmøte hos Oppdragsgiver, inkl. reisetid.
V3	Leverandør er ansvarlig for vedlikeholds- og serviceytelser frem til overtakelse.
V4	Leverandør er ansvarlig for feilretting av programvare gjennom anskaffelse og tilrettelegging av nye patcher, revisjoner eller versjoner som retter opp identifiserte feil
V5	Telefonsupport skal beskrives
V6	Det skal angis maksimal responstid ved akutte henvendelser. Det angis for ulike tider på døgnet og helger. Likeledes angis om anbyder har et vaktsystem for tilkalling utenom regulær arbeidstid. Eget telefonnummer for denne type support opplyses.
V7	Feilsøking/testprogrammer for vedlikehold skal inngå i leveransen
V8	Leverandøren skal beskrive hvilke rutiner firmaet har for oppgradering av programvare.

ID	Beskrivelse av krav
	Dokumentasjon
T1	Det vektlegges at Leverandøren fremlegger dokumentasjon som på en tydelig og oversiktlig måte viser de relevante hovedkomponenter, overordnet dataflyt og kommunikasjonsgrensesnitt internt og eksternt for løsningen. Dette kravet gjelder uavhengig av om løsningen består av kun programvare, kun enkeltstående MTU eller sammensatte løsninger med server(e), skytjenester, MTU(er) og klient-PCer for MTU-styring/overvåking og datahøsting fra MTU. Det er viktig at dokumentasjonen gjenspeiler løsningen, uansett størrelse og omfang, eksempelvis med en tilhørende illustrasjon, slik den er tenkt etablert hos Sykehuspartner. Dokumentasjonen skal inkludere alle enkeltkomponenter i løsningen (instrumenter, klient-PC, servere, lagring, nettverk, konvertere m.m.).
T2	Leverandøren skal fremlegge en detaljert oversikt over all relevant dataflyt over nettverk, slik den er planlagt etablert hos Sykehuspartner. Dette inkluderer detaljert dataflyt mellom løsningens enkeltkomponenter, med eksisterende tjenesteelementer i Sykehuspartners nettverk, samt eventuell datautveksling med skytjenester eller andre eksterne tjenester. Med «relevant» menes dataflyt over Sykehuspartners nettverk og derfor kan kreve at brannveggregler må tilrettelegges for at den tilbudte løsningen skal fungere i Sykehuspartners IKT-infrastruktur.
T3	Det IKT-relaterte bistandsomfanget i Leverandørens tilbud skal inkludere all leverandørbistand. Det omfatter ferdigstillelse av endelig løsningsdesign i Sykehuspartners infrastruktur, installasjon, konfigurasjon, testing og produksjonssetting, samt utarbeidelse av nødvendig løsning- og driftsdokumentasjon.
T4	Leverandøren bør forholde seg til, og etterleve, Sykehuspartners endringsregime for produksjonssatte løsninger.Det innebærer at leverandør kan ikke planlegge og/eller iverksette endringer som kolliderer med planlagte endringer i Sykehuspartners infrastruktur. Dette krever gjensidig varsling av planlagte endringer mellom aktørenes tjenesteansvarlige personell. Ved eventuell konflikt er det Sykehuspartners endringsregime som har prioritet.
T5	Den tilbudte løsningen bør bare benytte komponenter som har gyldige, produsentspesifikke vedlikeholdsavtaler gjennom hele kontraktsperioden. Komponenter som allerede er utenfor produsentspesifikk vedlikeholdsavtale (End Of Life/End Of Support) eller som vil bli det i løpet av avtaletiden skal spesifiseres.
T6	Leverandøren bør tilby en dokumentert og forpliktende roadmap for oppgradering og videreutvikling av den tilbudte løsningen. Langtidsplan og budsjett teller positivt.
T7	Leverandøren bør dokumentere at produsentens anbefalinger følges når det gjelder oppdatering og vedlikehold på tilbudt løsning.
T8	Den tilbudte løsningen bør kunne ivareta tiltenkt funksjon og/eller mellomlagre data lokalt på benyttet PC eller instrument ved brudd i nettverksforbindelsen. Beskriv hvordan.
T9	Beskriv maksimal tidsperiode for lokal lagringskapasitet/bufferkapasitet, samt hvilke overførings- og sletterutiner som eventuelt finner sted når datakommunikasjonen er gjenopprettet.
	Lisenser
T10	Eventuelle lisensieringsmekanismer bør være basert på sentral lisens og sentralisert lisensforvaltning.

T11	Leverandøren bør beskrive løsningens lisensieringsmekanismer, inklusiv leverandørens tekniske krav til dette. Dette inkluderer eksempelvis: • Bruk av lisensdongler eller andre fysisk tilkoblede enheter for lisensiering, samt tilkoblingsgrensesnitt (USB eller tilsvarende) • Bruk av klientlisenser som krever installasjon på Sykehuspartners arbeidsflate • Bruk av lisensserver, inklusiv leverandørens krav til denne • Bruk av lisensservere utenfor Sykehuspartners infrastruktur, inklusiv teknisk løsning og eventuelle konsekvenser for bruk av løsningen dersom slik kommunikasjon ikke kan etableres av Sykehuspartner.
T12	Utdyp begrensninger i bruk av løsningen som en konsekvens av lisensieringsmekanismen. Eksempler på viktige utdypingsområder er begrensninger av teknisk eller funksjonell art: • i antall brukere • samtidige brukere • i antall tilkoblede enheter • Lagringsvolumet • ved overskridelser av lisensgrenser
T13	Løsningen bør ha tydelige og veldokumenterte rutiner for forvaltning og vedlikehold av lisens. Eksempler på viktige utdypingsområder er: Hvordan fornyes evt. tidsavgrenset lisens Hvordan aktiveres/deaktiveres tidsbegrenset lisens Hvordan utføres versjonering av lisens
T14	Løsningen bør ved midlertidig bortfall av lisensieringsmekanisme fungere uten at dette påvirker bruken av løsningen. Leverandøren bes beskrive evt. konsekvenser for bruk av løsningen ved bortfall.
T15	Løsningen bør ha tydelige og veldokumenterte rutiner for forvaltning og vedlikehold av sertifikat(er). Eksempler på viktige utdypingsområder er: Hvordan fornyes evt. tidsavgrenset sertifikat Hvordan aktiveres/deaktiveres tidsbegrenset sertifikat Hvordan utføres versjonering av sertifikat
T16	Løsningen bør ha mekanisme/miljø for validering av at sertifikat som benyttes er gyldig.
	Nettverk
T17	Den tilbudte løsningen bør benytte industristandard teknologier/protokoller for datatrafikk. Gamle protokoller er en sikkerhetsrisiko, derfor vektlegges det at gamle protokoller unngås. Merknad: Utdyp eventuelle avvik.
T18	Den tilbudte løsningen skal benytte IPv4 og bør støtte IPv6. Den tilbudte løsningen skal konfigureres med Sykehuspartners egne IP-adresseserier dersom den har datautveksling over Ethernet/IP med Sykehuspartners systemer.
T19	Den tilbudte løsningen skal konfigureres med Sykehuspartners egne IP-adresseserier dersom den har datautveksling over Ethernet/IP med Sykehuspartners systemer.
T20	Dersom den tilbudte løsningen ikke støtter bruk av Sykehuspartners IP-adresseserier kan leveransen inkludere en dokumentert og leverandørdriftet ruter/gateway/brannmur som utfører "NAT/PAT" adresseoversetting mellom Sykehuspartners adresseserie og Leverandørens adresseserie. Dokumentasjonen skal inneholde nødvendige IP-adresser og TCP-/UDP-portnumre for tjenester som tilgjengeliggjøres. Denne ruter/gateway/brannmur-løsningen skal alltid risikovurderes og godkjennes før en tilkobling til Sykehuspartners nettverk kan utføres.
T21	Den tilbudte løsningen bør benytte Sykehuspartners nettverk uten å stille leverandørspesifikke begrensninger eller tekniske krav, utdyp eventuelle begrensinger. For eksempel i tilknytning til MDR/IVDR sertifisering.
T22	Den tilbudte løsningen bør håndtere brudd i nettverkskommunikasjon mellom de ulike delene av løsningen. Den medisinske funksjonaliteten bør opprettholdes mens systemet gjenoppretter sin nettverkskommunikasjon uten behov for manuelle brukeroperasjoner.

T23	Hvis den tilbudte løsningen implementerer dataoverføring basert på trådløs kommunikasjon bør det benyttes industristandard teknologier/protokoller. Utdyp eventuelle avvik gitt av leverandørspesifikke begrensninger eller tekniske krav, eksempelvis manglende support for sikkerhetsmekanismer, forholdsregler knyttet opp mot frekvenser, signalstyrker, mulig interferens etc.
T24	Leverandørens eventuelle lokale nettverk og Sykehuspartner sitt nettverk bør kunne sammenkobles. Dette må gjøres med Sykehuspartners godkjente ruter/brannmur som separerer den tilbudte løsningen fra Sykehuspartner sitt nettverk.
T25	Datatrafikk fra den tilbudte løsningen bør benytte IP-Unicast ved traversering av Sykehuspartners brannvegger. Det gjøres oppmerksom på at Sykehuspartners nettverk i dag ikke støtter bruk av IP-Multicast gjennom ruter/VRF.
T26	Leverandørens tilbudte løsning bør fungere uavhengig av WINS eller Windows hosts-fil.
	Klienter oig periferiutstyr
T27	Løsningen bør støtte nyeste Microsoft Windows versjon N-1
T28	Leverandørens løsning bør unngå bruk av komponenter med to eller flere nettverkskort.
T29	Leverandørens tilbudte løsning bør benytte periferiutstyr som skanner, strekkodeleser o.l. som kan leveres av Sykehuspartner. Spesifiser eventuelle leverandørspesifikke krav til slikt periferiutstyr (supporterte merker, modeller, strekkodeformater, utskriftsformat etc.).
T30	Leverandørens tilbudte serverløsning bør implementeres på virtuell serverplattform som kan leveres av Sykehuspartner. Utdyp leverandørens krav til virtuelle servere, for eksempel: RAM, CPU, OS (HOST/GUEST), disk, RAID, tilkoblingskort o.l.
	Operativsystem og programvare
T31	Leverandør bør utdype alle relevante krav til påkrevde 3.parts komponenter som leveres som en del av den tilbudte løsningen.
T32	Den tilbudte løsningens tilhørende klientapplikasjon(er) bør støtte standard Windows installer teknologi og være uten brukerinvolvering i installasjonsprosessen (s.k. silent installation). Teknologi som for eksempel Ivanti, App-V, msi og SCCM brukes i Sykehuspartner.
	Backup
T33	Backup av databaser bør kjøres mot eksisterende sentraliserte og automatiserte backuptjenester hos Sykehuspartner. Leverandøren gjøres oppmerksom på at backup-klient installeres på den tilbudte løsningen og eventuelle leverandørspesifikke brannmurer åpnes for tilgang fra Sykehuspartners backup-løsning.
T34	Databaser som inngår i den tilbudte løsningen, bør ha støtte for både full og inkrementell backup (gjennom f.eks. loggbackup/loggshipping) av databaser.
T35	Leverandørbistand ifm. gjenoppretting fra backup bør enten være inkludert eller spesifisert.
	Integrasjoner
T36	Den tilbudte løsningen bør inkludere API eller tekniske løsninger for å tilpasses en Integrasjonsløsning som er i henhold til industristandard innen helse, f.eks. HL7/FHIR. I påvente av API Infrastrukturen benyttes HSØ Integrasjonsplattform som en API Proxy med bruk av Microsoft Application Request Routing (ARR).
T37	Den tilbudte løsningen bør benytte API på en sikker måte for integrasjon og informasjonsutveksling. Dokumenter hvilke sikkerhetsmekanismer den tilbudte løsningen kan supportere ved bruk av API.
T38	All informasjonsutveksling bør etableres i henhold til industristandard. Eksempler på slike standarder er HL7/FHIR og DICOM, se Direktoratet for e-helse
T39	Den tilbudte løsningen bør benytte Sykehuspartners standardiserte integrasjonstjeneste. Det bør ikke stilles leverandørspesifikke krav eller begrensninger for semantikk i de benyttede standardiserte meldingsformater, inkludert hvilke formatversjoner, som kan benyttes. Spesifiser eventuelle krav/begrensninger, inkludert eventuelle implementeringsavvik i benyttet standard. Eksempler på slik semantikk er: ASTM, HL7, ebXML.

T40	Den tilbudte løsningen bør ha mulighet for logging av meldingsflyt og meldingskvitteringer. Hensikten er å oppdage meldinger som ikke kommer frem eller blir kvittert med negativ kvittering, og hvilke meldinger som har kommet korrekt fram til mottakeren. Beskriv hvilken loggfunksjonalitet den tilbudte løsningen eventuelt har og hvordan dette kan understøtte behov for meldingsdokumentasjon. Dokumentasjonen bes inkludere eventuell feilsøking og analysering av avvik på sendte og mottatte data i grensesnittet mellom MTU og andre aktører.
T41	Den tilbudte løsningen bør leveres med dokumentasjon som beskriver leverandørens grensesnitt for integrasjoner.
	Databehandling og leverandørstyring
T42	Leverandør skal tydelig informere om, og skriftlig dokumentere, den geografiske lokasjonen (land) der behandling av personopplysninger skjer. Med behandling menes blant annet prosessering, lagrede data, fjernaksess, support/vedlikehold, sletting og data i transport.
T43	Alt innleid personell, samt leverandører som utfører tidsbegrenset arbeid på vegne av virksomheten bør signere sikkerhetsinstruks
T44	Leverandøren bør akseptere å benytte kundens mal for databehandleravtale. Dersom annen databehandleravtale skal brukes, må leverandøren opplyse om avvik mellom kundens og leverandørens mal.
T45	Leverandøren bør kunne dokumentere egen informasjonssikkerhet iht. ISO 27001, eller tilsvarende. Ved sertifisering bør SOA (Statement of Applicability) vises til.
T46	Leverandørens tilgang til tjenesten bør kun gå via Sykehuspartners leverandørportal og ikke direkte til komponenter i Sykehuspartners infrastruktur via eks. VPN fra leverandørens enheter. Leverandør bes beskrive hvordan tilgang kan gjøres.
T47	Ved support bør relevant materiell/logger tilgjengeliggjøres via Sykehuspartners leverandørportal eller filsluse.
T48	Løsning med underliggende komponenter bør supporteres i kontraktsperiodens levetid. Leverandøren må opplyse om forventet levetid for alle komponenter.
T49	Leverandør og underleverandør skal bekrefte at de er kjent med kravene i personopplysningsloven/GDPR og etterlever Norm for informasjonssikkerhet og personvern i helse og omsorgstjenesten (Normen).
T50	Leverandør skal bidra med informasjon om hvordan de behandler personopplysninger på vegne av dataansvarlig.
	Identifisering
T51	Løsningen bør ikke benytte lokale brukerdatabaser, men Helse Sør-Østs identiteter. Leverandøren bes beskrive hvordan
T52	Det bør kun benyttes personlige brukere. Avvik fra dette og eventuelle behov for fellesbrukere må beskrives.
T53	Løsningen bør støtte at flere roller og/eller organisasjoner er assosiert med samme unike bruker-ID. Tilgang kan differensieres etter hvor den ansatte arbeider til enhver tid.
	Autentisering
T54	Løsningen bør kunne benytte Helse Sør-Østs autentiseringstjeneste (Eksternalisert autentisering). Leverandøren bes beskrive hvordan løsningen autentiserer alle typer brukere, ping federate prefereres.
T55	Løsningen bør ha støtte for føderering, preferert er Open ID Connect. Leverandøren bes beskrive hvilke protokoller løsningen benytter.
T56	Regelmessige og planlagte oppgaver på løsningen bør kjøres av servicekontoer. Servicekontoer bør standardiseres og herdes iht. anerkjente standarder.
T57	På tidspunktet brukeren logger inn, bør applikasjonen autorisere tilgang, opprette en sikkerhetsøkt og logge brukeraktiviteter basert minst på bruker-ID, organisasjonsenhet og rolle.

T58	Applikasjonen bør håndheve og vedlikeholde en sikkerhetsøkt for sluttbrukeren.
	Autorisering
T59	Brukerkontoer i løsningen bør ikke gis administrative rettigheter. For behovsbaserte formål bør separate personlige adminkontoer, dvs at brukere som skal utføre administrative oppgaver får en egen brukerkonto med aktuelle rettigheter som kun benyttes til admin-formål.
T60	Løsningen bør ha støtte for rollebasert tilgangsstyring ("RBAC"/"PBAC"). Tilgang til funksjonalitet og pasientdata bør kunne sammenstilles for å begrenses tilganger, eks. rolle og organisasjonstilhørighet.
T61	Beskriv alle roller som finnes i løsningen, med tilhørende rettighetsnivå og hvordan disse forvaltes. Eksempel på roller kan være superbruker, adminbruker, kliniker, tekniker.
	Sporbarhet
T62	Logger som leverandør har tilgang til for drift og forvaltning bør kun inneholde teknisk informasjon, og ikke personopplysninger.
T63	Alle relevante handlinger bør logges og kunne tilgjengeliggjøres for gjennomgang. Som et minimum er dette: · Alle typer innlogginger, inkl. forsøk på innlogginger · Oppretting, endring og sletting av informasjonsobjekter · Oppretting, endring og sletting av andre brukere · Innsyn eller endring i personopplysninger · Endringer, eller forsøk på endringer, i systemkonfigurasjonen Beskriv hvordan dette ivaretas i tilbudt løsning.
T64	Relevante sikkerhetslogger bør logges i standardisert format (RFC 5424) og kunne overføres til sentralt loggmottak (Splunk).
T65	Logger som lagres i løsningen bør tilgangsstyres, beskriv hvordan dette ivaretas i løsning.
T66	Logger bør være tidssynkronisert mot sentral NTP-tjeneste.
T67	Løsning bør kunne lagre logger i minimum 24 mnd. Beskriv hvordan dette ivaretas for de forskjellige typene logger i løsning.
	Infrastruktur
T68	Løsningens infrastruktur (klienter/servere/databaser) bør være bygd slik at kommunikasjon initieres fra det høyeste tillitsnivået. Leverandøren bes dokumentere alle komponenter med retning på trafikk initiering. Høyeste nivå er nivået med høyest beskyttelsesbehov og ofte der data lagres permanent.
T69	Leverandøren bør ha oversikt over og dokumentert, alle porter og protokoller som kreves for at tjenesten kan kjøres på et optimalt nivå. Hver enkelte portåpning skal ha et dokumentert behov. Portåpninger skal holdes på et minimumsnivå. Porter som benyttes bør inngå i arkitekturbeskrivelse av løsning.
T70	Løsningen med tilhørende IKT-komponenter bør tåle at det benyttes nettverksbasert sårbarhetsscanning. Leverandør bes beskrive potensiell ytelseskonsekvens av sårbarhetsscanningen.
	Klientsikkerhet

T71	Løsningen bør benytte klienter levert av Sykehuspartner. Dersom dette ikke kan etterleves gjelder følgende: • Klienter bør ha kryptert harddisk • Klienter bør ha automatisk installasjon av sikkerhetsoppdateringer • Klienter bør ha antivirusprogram med jevnlig oppdatering av antivirussignaturer. • Klienter bør ha automatisk låsing av skjerm m/ passord, • Brukere bør ikke ha administrasjonsprivilegier på egen klient. Brukere bør ikke kunne deaktivere lokale sikkerhetskontroller • Klienter bør kun ha godkjent og risikovurdert programvare installert • Klienter bør autentiseres gjennom klientsertifikater for å kunne koble seg på Virksomhetens nettverk. • Klienten bør herdes i tråd med beste praksis. Det anbefales at CIS' Benchmark brukes som rammeverk for herding. Der hvor CIS' Benchmark ikke kan benyttes, må det fremkomme. • Antivirus scanning bør skje automatisk og uten behov for ekskludering av mapper. Leverandøren må ta stilling til alle overstående punkter, og beskrive dette i sin besvarelse.
	Serversikkerhet
T72	Løsningen bør benytte servere/databaser levert av Sykehuspartner. Dersom dette ikke kan etterleves gjelder følgende: • Server bør herdes i tråd med beste praksis. Det anbefales at CIS' Benchmark brukes som rammeverk for herding. Der hvor CIS' Benchmark ikke kan benyttes, må det fremkomme. • Serveren bør ha installert gjeldende sikkerhetsoppdateringer og antivirussignaturer. • Serveren bør inngå i driftsovervåkingen. • Serveren bør synkronisere klokken mot sentral NTP-server • Bruk av ressurser bør inn i regime for overvåking og justering, og det bør foretas beregninger over framtidige kapasitetsbehov for å sikre at systemet oppnår påkrevd ytelse • Servere bør benytte Sykehuspartners standard programvare for antivirus • Antivirus scanning bør skje automatisk og uten behov for ekskludering av mapper. Leverandøren må ta stilling til alle overstående punkter, og beskrive dette i sin besvarelse.
	Appliksjonssikkerhet
T73	Løsning bør legge til rette for effektiv og hurtig installasjon av sikkerhetsoppdateringer. Leverandør bes beskrive prosess for oppdateringer av alle komponenter i løsning. Dette innebærer også om det er kunden eller leverandøren som er ansvarlig for oppdateringer og hvordan oppdateringer/patcher tilgjengeliggjøres for kunden.
T74	Løsningen bør benytte en trelagsarkitektur for å begrense eksponering av lagret data.
T75	Foretrukket løsning for utskrift er basert på sentraliserte nettverksskrivere med «Pull Print» (sikker print). Leverandørens tilbudte løsning bør benytte sentraliserte nettverksskrivere som kan leveres av Sykehuspartner.
T76	Løsning bør ha støtte for kryptering av data under transport og som minimum benytte TLS 1.2. Kryptering mellom alle komponenter i løsning må beskrives. Dette bør inngå i dokumentert skisse av løsning.
T77	Løsning bør ha støtte for kryptering av data under lagring. Krypteringsmetode må beskrives.
T78	Beskriv alle protokoller som benyttes for å utveksle informasjon i løsningen. Det bør ikke benyttes protokoller med kjente sårbarheter (eks SMB v.1). Protokoller som benyttes bør fremkomme av dokumentasjon.
T79	Personopplysninger bør ikke overføres i parametere, metadata, header eller på annet vis i integrasjoner slik at de blir synlige i transportlogger underveis til mottakeren. F.eks ved bruk av HL7 FHIR GET vil parameterne legges i webserver loggen på transportserverne"
T80	Løsningen bør benytte sentralisert fillager/ database. Det er ønskelig å kunne lagre data fra flere dataansvarlige sammen, med logiske skiller mellom data. Mulighet for dette må beskrives.

T81	Løsningen bør benytte sentralisert fillager/ database. Det er ønskelig å kunne lagre data fra flere dataansvarlige sammen, med logiske skiller mellom data. Mulighet for dette må beskrives.
T82	Leverandørens tilbudte løsning bør være kompatibel med bruk av IEEE 802.1x (Network Access Control). For alt utstyr som skal tilkobles og gis tilgang til Sykehuspartners nettverk, registreres utstyret som hovedregel med godkjent MAC-adresse for tilgangskontroll.
T83	Ved behov for bruk av eksterne lagringsenheter bør den tilbudt løsningen støtte kryptering av data.
	Skykrav
T84	Ansvar for sikkerhetstiltak følger av ansvarsmatrisen, se over. Der det er delt ansvar skal leverandøren beskrive hva de er ansvarlig for.
T85	Leverandøren skal vedlegge utfylte CAIQ. Tilbyders CAIQ kan gjerne være basert på underleverandørs/skyleverandørens CAIQ, der det er relevant, for å sikre en god besvarelse.
T86	Alle leverandører og underleverandører som skal behandle personopplysninger bør kunne dokumentere egen sikring av personopplysninger iht. ISO 27017; ISO27018 eller tilsvarende. Ved sertifisering bør SOA (Statement of Applicability) vises til.
T87	Ved endringer i leverandørens standardvilkår, skal leverandøren varsle Sykehuspartner slik at Sykehuspartner kan ta stilling til endringen
T88	Leverandøren skal til enhver tid ha oversikt over alle aktuelle underleverandører i leverandørkjeden som er relevant for tjenesten. Verdikjeden av databehandling i tjenesten skal være skriftlig dokumentert, herunder hvilke opplysninger som behandles av den aktuelle leverandøren. Oversikten kan ligge i et bilag i en databehandleravtale, eller på en nettside. Eventuelt skal leverandøren på oppfordring fra Sykehuspartner kunne presentere en oversikt over alle underleverandører og tjenester disse yter for aktuell avtale.
T89	Dersom behandling av personopplysninger vil skje utenfor EU/EØS, og godkjente tredjeland, bør Transfer Impact Assessment (TIA) vedlegges.
T90	Leverandøren bør sikre at personopplysninger fra ulike dataansvarlige skilles, enten fysisk eller logisk. Leverandøren bes beskrive hvordan dette kan ivaretas.
T91	Leverandør bør beskrive hvilke sikkerhetsmekanismer de benytter for å beskytte data.
T92	Løsningen bør ha mulighet for å minimum benytte autentiseringsnivå betydelig (Mobilbasert MFA, BuyPass, BankID)
T93	Leverandørs bruk av administrative- eller privilegerte tilganger bør spores og logges.
T94	Leverandørens administrative tilganger i skytjenesten bør i størst mulig grad begrenses. Just-in-Time-Access skal benyttes om mulig.
T95	Leverandør bør dokumentere at fysisk sikring, inkludert perimetersikring og adgangskontroll, er i henhold til etablerte anerkjente standarder eller rammeverk som omtaler sikring av datasenter (f.eks ISO TS 22237, ISO27001, CSA Star certification, PCI DSS mv.)
T96	Leverandør skal gjøre nødvendige logger umiddelbart tilgjengelig for Sykehuspartner CERT, ved forespørsel.
T97	Hendelser som påvirker skytjenestens ivaretagelse av konfidensialitet, integritet eller tilgjengelighet skal meldes gjennom avtalt grensesnitt, uten ugrunnet opphold, til Sykehuspartner CERT.
T98	Sikkerhetstesting bør inkluderes i tjenesteleveransen, og det bør være etablerte prosesser for å identifisere sårbarheter (ikke begrenset til): Sårbarhetsscanning Penetrasjonstester Vurdere sårbarheter Håndtere sårbarheter Leverandøren bes beskrive hvilke, og hvordan, prosessene gjennomføres.

T99	Eierskap og forvaltning av krypteringsnøkler bør være avklart. Leverandør bes beskrive hvordan dette ivaretas.
T100	Utviklings-, test- og produksjonsmiljøer bør skilles fysisk og/eller logisk. Beskriv hvordan miljøene er satt opp og skille mellom de.