

## **Bilag 3A til vedlegg 5**

Kundens tekniske plattform HSØ

Innovasjonspartnerskapet

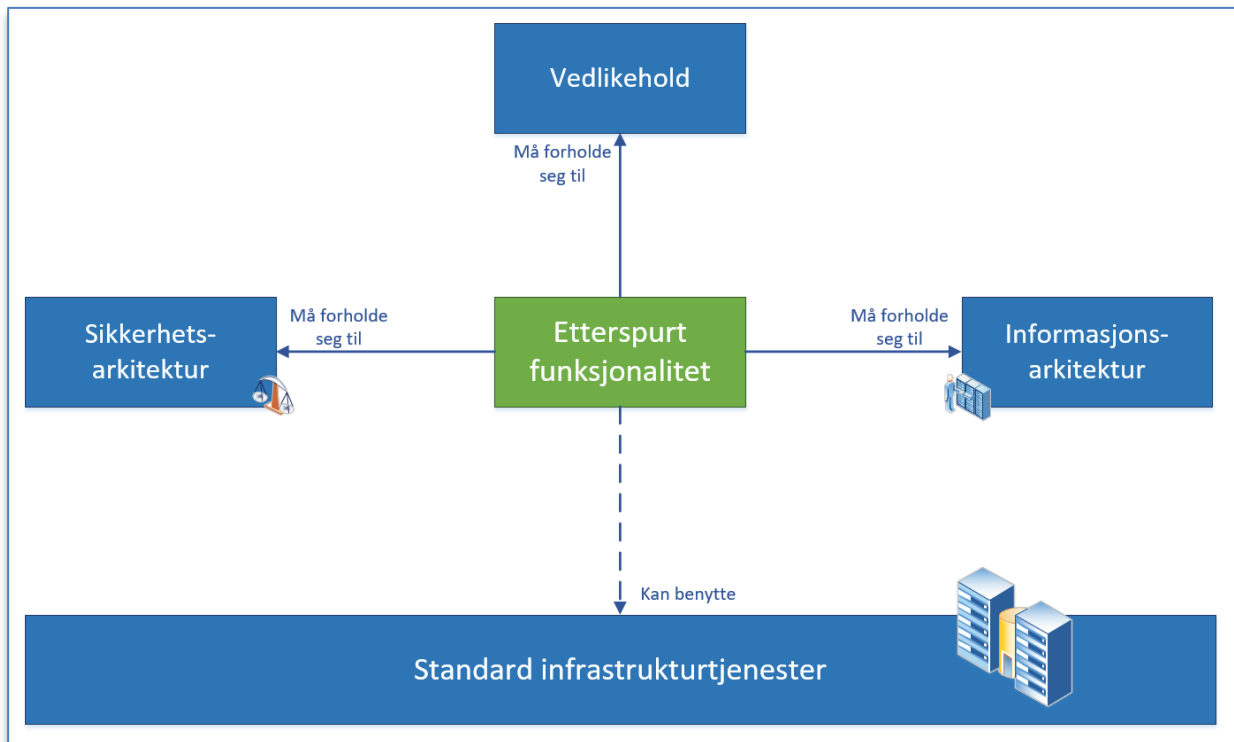
**«Sikker prøvetaking og analyse i hjemmet  
utført av pasient»**

## Innholdsfortegnelse

<b>1</b>	<b>Introduksjon</b> .....	<b>3</b>
<b>2</b>	<b>Arkitekturprinsipper</b> .....	<b>3</b>
2.1	Skybasert.....	3
2.2	Informasjonsdeling .....	4
2.3	Grønn IT .....	4
<b>3</b>	<b>Sikkerhet</b> .....	<b>4</b>
3.1	Tilgangsstyring .....	4
3.2	Tilgangslogging .....	4
3.3	Integritet.....	4
3.4	Tilgjengelighet .....	4
<b>4</b>	<b>Integrasjon</b> .....	<b>4</b>
4.1	Tjenesteorientering.....	4
4.2	Autoritative kilder .....	5
4.3	Identitet og tilgangsstyring.....	5
<b>5</b>	<b>Grunnleggende infrastrukturtjenester og vedlikeholdbarhet</b> .....	<b>5</b>
5.1	Standardisering .....	5
5.2	Leverandørtilgang.....	5
5.3	Lifecycle Management.....	5
5.4	Virtualisering .....	5
5.5	Applikasjonsdistribusjon .....	6

## 1 Introduksjon

Sykehuspartner søker på vegne av Helse Sør-Øst at løsninger som anskaffes tilfredsstillende grunnleggende krav som dekker sikkerhet, integrasjon og vedlikeholdbarhet. Dette dokumentet fremstiller de overordnede prinsippene som gjelder på disse områdene.



## 2 Arkitekturprinsipper

Helse Sør-Øst mener det er visse egenskaper som er viktige for alle løsninger som skal innføres. Disse egenskapene er nedfelt som arkitekturprinsipper. Løsninger som skal anskaffes vurderes opp mot deres evne til å tilfredsstille de mest grunnleggende av disse prinsippene.

Prinsippene nærmere beskrevet i følgende dokumenter:

- [DIFIs «Overordnede IT arkitekturprinsipper for offentlig sektor»](#)
- [DIFIs «Arkitekturprinsipper for samhandling»](#)
- [Nasjonal IKT «Arkitekturprinsipper i spesialisthelsetjenesten»](#)

### 2.1 Skybasert

Helse Sør-Øst anser at skytjenester kan gi stor verdi for løsninger som skal tilbys helseforetakene. Sykehuspartner HF leverer tjenester produsert i egen, privat sky, samt som broker fra eksterne, offentlige skytjenester. Prinsippene for skybaserte løsninger er tydeligst uttrykt i NIST standarden:

- Behovsbasert
- Levert over nett
- Delte ressurser
- Umiddelbar fleksibilitet
- Betaling etter bruk

## 2.2 Informasjonsdeling

Helse Sør-Øst ønsker å legge til rette for at informasjon fra fagsystemene gjøres tilgjengelig til brukere der disse måtte befinne seg på en sikker måte. Det betyr at Helse Sør-Øst erkjenner at for enkelte typer informasjon så vil det være nødvendig at denne kan deles med individer som ikke er ansatt i Helse Sør-Øst og som derfor heller ikke har Helse Sør-Øst definert utstyr eller tilgang til Helse Sør-Øst sine lokasjoner.

## 2.3 Grønn IT

Helse Sør-Øst ønsker å fremme bærekraftig bruk av IT og trenger derfor informasjon om hvordan den enkelte løsning understøtter dette gjennom sin livssyklus. Dette gjelder både bruk av råmaterialer, energi og menneskelige ressurser både hos leverandøren og eventuelle underleverandører.

## 3 Sikkerhet

Sikkerhet omfatter konfidensialitet, integritet og tilgjengelighet. Gitt at løsninger som anskaffes til bruk i helseforetakene i de fleste tilfeller vil behandle sensitiv informasjon så har Helse Sør-Øst over tid gjennomført tiltak og etablert standarder for hvordan behov for sikker tilgjengeliggjøring av informasjon dynamisk kan balanseres opp mot risiko for pasientsikkerheten.

### 3.1 Tilgangsstyring

Helse Sør-Øst har etablert en IAM løsning som tilbyr rolle- og attributtbasert tilgangsstyring. Tilgang til informasjon styres gjennom Helse Sør-Øst sin IAM løsning. Det betyr at en applikasjon må forholde seg til en eksternalisert identitet for både autentisering og autorisering.

*Tjenester for tilgangsstyring beskrives i eget vedlegg (Bilag 3c – Identitet og tilgangsstyring)*

### 3.2 Tilgangslogging

Helse Sør-Øst er pålagt å følge opp tilgang til pasientinformasjon. Dette gjøres ved at tilganger logges og at slike logger analyseres gjennom Helse Sør-Øst sin Logganalyseløsning. All tilgang gis basert på personlig identitet.

### 3.3 Integritet

Løsningens integritet omfatter evnen til å sikre at feil ikke påvirker datagrunnlaget i løsningen. Bruker- og systemendringer på data som er kritisk for eks. pasientbehandling skal logges og kunne avleveres til Helse Sør-Øst sin Logganalyseløsning.

### 3.4 Tilgjengelighet

Alle aktuelle brukergrupper skal ha tilgang til nødvendig funksjonalitet og informasjon i rett form til rett tid og på rett sted. Tjenester og løsninger som anskaffes må kunne tilfredsstillende Helse Sør-Øst sitt krav til tilgjengelighet.

## 4 Integrasjon

### 4.1 Tjenesteorientering

Helse Sør-Øst har en tjenesteorientert integrasjonsarkitektur der ulike fagsystemer tilbyr og konsumerer tjenester på integrasjonsplattformen gjennom synkroner tjenester. Tjenesteorienteringen skal bidra til å forbedre samhandling mellom systemer og gi en lavere

terskel for nye systemer til å tilby funksjonalitet. Det er ikke ønskelig at fagsystemer har egne integrasjonsløsninger som overlapper med Helse Sør-Øst integrasjonsplattform.

*Integrasjonstjenester er beskrevet i bilag 3b - integrasjon*

## 4.2 Autoritative kilder

Helse Sør-Øst har etablert prinsipper for autoritative kilder som nye løsninger må forholde seg til. Dette betyr at leverandørens løsning må forholde seg til at sentrale dataelementer i egen løsning oppdateres utenfor løsningen og at løsningen må håndtere og hente slike dataelementer fra kilden samt at eventuelle oppdateringer skal gjøres via kilden.

## 4.3 Identitet og tilgangsstyring

Integrasjoner er gjenstand for de samme sikkerhetskrav som brukertilganger generelt. Det betyr at fagsystemers bruk av integrasjoner må autentiseres, autoriseres og loggføres samt at overføring av informasjon mellom fagsystemer og integrasjonsplattform må krypteres.

# 5 Grunnleggende infrastrukurtjenester og vedlikeholdbarhet

## 5.1 Standardisering

Sykehuspartner leverer et sett med infrastrukurtjenester. Disse tjenestene utgjør de grunnleggende byggesteinene som benyttes for å sette sammen applikasjonstjenester for helseforetakene. Tjenestene leveres fra regionale datasentre til avtalte enhetspriser per tjenestenivå.

*Infrastrukurtjenester er beskrevet i bilag 3a – Standard infrastruktur.*

## 5.2 Leverandørtilgang

En leverandør som skal levere en løsning basert på Helse Sør-Øst sine infrastrukurtjenester vil få tilgang til administrasjonsgrensesnitt for løsningen gjennom en standard Leverandørtilgangstjeneste for privilegert tilgang. Grunnleggende for denne tjenesten er at leverandørens brukere skal ha personlig identitet og at autentisering og autorisering følger Helse Sør-Øst IAM retningslinjer. Federering av leverandørens IAM løsning med Helse Sør-Øst's IAM løsning vil foretrekkes. Leverandørens tilganger vil logges da det kan være sensitiv informasjon i løsningen.

## 5.3 Lifecycle Management

Helse Sør-Øst er opptatt av at løsninger skal kunne vedlikeholdes og videreutvikles løpende, såkalt Lifecycle Management. Man har som føring at software<sup>1</sup> støttes i gjeldende hovedversjon samt at også forrige hovedversjon skal støttes (N, N - 1). Merk at dette medfører at løsningen må understøtte løpende patching samt at leverandøren må kontinuerlig oppdatere sin løsning til å støtte nye hovedversjoner av tilstøtende komponenter når disse gjøres tilgjengelig i markedet. Typisk her er nye versjoner av operativsystemer, databaser, nettlesere og tilknyttede elementer til disse.

## 5.4 Virtualisering

Helse Sør-Øst har som strategi å virtualisere sine løsninger, og applikasjoner som kan virtualiseres både på server og klient vil bli preferert.

<sup>1</sup> Software omfatter både leverandørens løsning, underliggende operativsystem og andre støttefunksjoner som en tjeneste bygger på.

## 5.5 Applikasjonsdistribusjon

Helse Sør-Øst har en strategi for virtualisering av brukergrensesnittet. Helse Sør-Øst tilbyr distribusjon av applikasjoner tilpasset brukerens og applikasjonens behov samt den situasjon tilgang ønskes i. Det prefererte grensesnittet er web basert. Skal en applikasjon installeres på klientutstyr så må denne kunne pakkes og distribueres automatisk, og tykke<sup>2</sup> og tynne<sup>3</sup> klienter samt strømming av installasjonen må støttes.

---

<sup>2</sup> 'Tykk' betyr her tradisjonell applikasjonsdistribusjon i form av lokal installasjon av applikasjonen på brukerens utstyr.

<sup>3</sup> 'Tynn' betyr her applikasjonsdistribusjon i form av tynnklientløsninger så som RDP eller ICA.