**Risikovurdering**

**PROSJEKTFORMALIA:**

|  |  |
| --- | --- |
| Prosjektets navn |  |
| Tjenestens navn |  |
| Tjenesteansvarlig |  |
| Regional/lokal systemeier |  |
| Prosjektnummer |  |
| Prosjektleder |  |
| Leveransekoordinator |  |
| Godkjenner av tilbud HF |  |
| Løsningsdesigner |  |
| Risikobehandler |  |
| Berørt(e) helseforetak |  |
| Sikkerhetsleder(e) på berørt(e) foretak |  |

**ENDRINGSHISTORIKK:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Versjon | Dato | Kapittel | Endring | Versjon av Løsningsdesign | Endring utført av |
|  |  |  |  |  |  |

**Rapport utarbeidet av [Sett inn]**

Dato

Forord

Denne risikovurderingsrapporten beskriver løsningens risikobilde basert på forelagt saksgrunnlag. Følgende elementer dekkes:

* Omfang og avgrensinger i risikovurderingen.
* Beskrivelse av grunnlaget for risikovurderingen.
* Etterlevelse av krav til løsningen.
* Kartlegging av mulige sårbarheter og tilhørende trusselscenarier.
* Vurdering av risiko, herunder sannsynlighet og konsekvens.
* Kartlegging av relevante tiltak i de tilfeller der anslått risiko er høyere enn akseptabel risiko.

**Hensikten med denne rapporten**

Hensikten med risikovurderingen er å dekke lovpålagte krav[[1]](#footnote-1) som sier at risikovurdering skal gjennomføres ved ny innføring og endring som har betydning for informasjonssikkerhet. Risikovurderingen har også nytteverdi i form av identifikasjon av risiko, og anbefaling av konkrete risikoreduserende tiltak knyttet opp mot identifiserte sårbarheter.

**Behandling av anbefalte tiltak**

For å sikre god håndtering av identifiserte risikoer, anbefales det å ha et aktivt forhold til de fire T-ene for risikohåndtering.

|  |  |
| --- | --- |
| **Tolerate**  (Akseptere) | Det er ikke mulig å fjerne all risiko. Noe risiko kan derfor aksepteres, men det er viktig at risikoen er identifisert, forstått og akseptert av berørte parter. Vurdering av kost/nytteverdi vil være sentral i denne sammenheng. Merk at etterlevelse av lovpålagte krav kan ikke være gjenstand for en slik vurdering, og at avvik ikke aksepteres. |
| **Treat**  (Behandle) | Iverksette tiltak for å redusere risikoen, enten ved å redusere sannsynligheten for at den inntreffer eller ved å redusere konsekvensene det vil medføre at risikoen inntreffer. |
| **Transfer**  (Overføre) | Noe av den finansielle risikoen kan muligens overføres til forsikringsselskap, gjennom kontraktsmessige forhold med en tredje part, eller ved at mulige berørte parter aksepterer den risikoen de kan bli påført. Merk at overføring av risiko knyttet til sensitiv informasjon i liten grad vil være et alternativ. |
| **Terminate**  (Fjerne) | Dersom en identifisert risiko anses som uakseptabel og denne ikke kan kontrolleres, behandles eller overføres, kan løsningen være å eliminere alle aktiviteter/elementer som påfører denne risikoen. |

**Behandling av risikovurderingen**

Som databehandleransvarlig er det berørt helseforetak som kan beslutte tjenestens risikoakseptnivå. Risikovurderingsrapporten med anbefalte tiltak skal legges frem for sikkerhetsleder i berørt Helseforetak for aksept av risikonivå. Ved regionale løsninger, som innebærer at samme tjeneste og samme database benyttes av to eller flere helseforetak, skal risikovurderingen behandles regionalt av det Regionale Risikovurderingsteamet.

Helseforetaket er juridisk eier av risikovurderingen og må sikre at dokumentasjonen behandles forskriftsmessig i henhold til lovkrav og gjeldende rutiner.

Innhold

[1 Sammendrag 4](#_Toc462743675)

[2 Introduksjon og avgrensninger 5](#_Toc462743676)

[2.1 Beskrivelse av nytt system 5](#_Toc462743677)

[2.2 Oversikt over funksjonalitet i løsningen 5](#_Toc462743678)

[2.3 Klassifisering av opplysninger og krav til informasjonsbehandling 5](#_Toc462743679)

[2.4 Klassifisering av tilgjengelighet 5](#_Toc462743680)

[2.5 Omfang og avgrensing av risikovurderingen 5](#_Toc462743681)

[2.6 Aktører og overordnet beskrivelse av deres rolle 5](#_Toc462743682)

[3 Grunnlag for risikovurderingen 6](#_Toc462743683)

[3.1 Arkitekturbeskrivelse 6](#_Toc462743684)

[3.1.1 Overordnet teknisk realisering 6](#_Toc462743685)

[3.1.2 Teknologi brukt i løsningen 6](#_Toc462743686)

[3.1.3 Dataflyt med integrasjoner 6](#_Toc462743687)

[3.2 Avvik og innspill til risikomomenter 6](#_Toc462743688)

[3.2.1 Avvik fra etablerte prinsipper 6](#_Toc462743689)

[3.2.2 Innspill til risiko 6](#_Toc462743690)

[3.3 Konfidensialitet, lagring, tilgang og transport 6](#_Toc462743691)

[3.3.1 Informasjonstyper i løsningen 6](#_Toc462743692)

[3.3.2 Bruk av informasjonsaktiva 6](#_Toc462743693)

[3.4 Konfidensialitet, kryptering og bruk av sertifikater 6](#_Toc462743694)

[3.4.1 Applikasjonskryptering 6](#_Toc462743695)

[3.4.2 Nettverkskryptering 6](#_Toc462743696)

[3.4.3 Kryptering av lagringsmedier 6](#_Toc462743697)

[3.4.4 Bruk og forvaltning av sertifikater 6](#_Toc462743698)

[3.5 Tilgangsforvaltning 6](#_Toc462743699)

[3.5.1 Autentisering, beskrivelse av mekanisme 6](#_Toc462743700)

[3.5.2 Autorisering, beskrivelse av definerte roller i løsningen 6](#_Toc462743701)

[3.5.3 Forvaltning av autentisering i løsningen 6](#_Toc462743702)

[3.5.4 Forvaltning av autorisering i løsningen 6](#_Toc462743703)

[3.6 Leverandørtilgang 6](#_Toc462743704)

[3.6.1 Leverandør autorisering 6](#_Toc462743705)

[3.6.2 Leverandør autentisering 6](#_Toc462743706)

[3.6.3 Kryptering av leverandørforbindelser 6](#_Toc462743707)

[3.6.4 Taushetserklæring og databehandleravtale 6](#_Toc462743708)

[3.7 Pasientens konfidensialitetsrettigheter, sperring 6](#_Toc462743709)

[3.7.1 Lovpålagt forankring 6](#_Toc462743710)

[3.7.2 Beskrivelse av sperremekanisme 6](#_Toc462743711)

[3.8 Pasientens konfidensialitetsrettigheter, logging og logghåndtering 7](#_Toc462743712)

[3.8.1 Beskrivelse av etablert løsning for logging 7](#_Toc462743713)

[3.8.2 Oppbevaring og forvaltning av logger 7](#_Toc462743714)

[3.8.3 Tilgangskontroll av logger 7](#_Toc462743715)

[4 Risikovurdering 8](#_Toc462743716)

[4.1 Krav til løsningen og etterlevelse 8](#_Toc462743717)

[4.1.1 Etterlevelse av sikkerhetsprinsipper og -krav for IKT 8](#_Toc462743718)

[4.1.2 Etterlevelse av foretaksspesifikke krav 8](#_Toc462743719)

[4.2 Mulige sårbarheter og tilhørende trusselscenarier 9](#_Toc462743720)

[4.3 Vurdering av risiko 10](#_Toc462743721)

[5 Anbefalte risikoreduserende tiltak 11](#_Toc462743722)

[VEDLEGG A: Besvart etterlevelse av Sikkerhetsprinsipper og -krav for IKT 12](#_Toc462743723)

[VEDLEGG B: Andre involvert personer i risikovurderingen 20](#_Toc462743747)

[VEDLEGG C: Referanser 21](#_Toc462743748)

[VEDLEGG D: Helseforetakets behandling 22](#_Toc462743749)

# Sammendrag

Rapporten beskriver risikoforhold knyttet til informasjonssikkerhet som er identifisert i løsninger levert av .

Det er identifisert mulige trusselscenarier og hendelser basert på mulige sårbarheter. av risikoene er utenfor akseptansegrensen (gule) og krever oppfølging og vurdering av prosjektet og helseforetaket. av risikoene er uakseptable (røde). Det er anbefalt risikoreduserende tiltak.

De viktigste risikoreduserende tiltakene er gjengitt i oversikten under:

|  |  |
| --- | --- |
| *Beskrivelse av tiltak* | *Anbefalt ansvarlig for behandling av tiltak* |
|  |  |
|  |  |

# Introduksjon og avgrensninger

Kapittel 2 gir en kort introduksjon til løsningen, samt omfang og avgrensinger i risikovurderingen.

## Beskrivelse av nytt system

## Oversikt over funksjonalitet i løsningen

## Klassifisering av opplysninger og krav til informasjonsbehandling

## Klassifisering av tilgjengelighet

## Omfang og avgrensing av risikovurderingen

## Aktører og overordnet beskrivelse av deres rolle

# Grunnlag for risikovurderingen

Kapittel 3 beskriver grunnlaget for risikovurderingen. All beskrivelse av løsningen er en direkte tekstlig og visuell gjengivelse fra løsningsdesignet. Ved behov for utfyllende beskrivelse av løsningen henvises det til løsningsdesignet.

## Arkitekturbeskrivelse

### Overordnet teknisk realisering

### Teknologi brukt i løsningen

### Dataflyt med integrasjoner

## Avvik og innspill til risikomomenter

### Avvik fra etablerte prinsipper

### Innspill til risiko

## Konfidensialitet, lagring, tilgang og transport

### Informasjonstyper i løsningen

### Bruk av informasjonsaktiva

## Konfidensialitet, kryptering og bruk av sertifikater

### Applikasjonskryptering

### Nettverkskryptering

### Kryptering av lagringsmedier

### Bruk og forvaltning av sertifikater

## Tilgangsforvaltning

### Autentisering, beskrivelse av mekanisme

### Autorisering, beskrivelse av definerte roller i løsningen

### Forvaltning av autentisering i løsningen

### Forvaltning av autorisering i løsningen

## Leverandørtilgang

### Leverandør autorisering

### Leverandør autentisering

### Kryptering av leverandørforbindelser

### Taushetserklæring og databehandleravtale

## Pasientens konfidensialitetsrettigheter, sperring

### Lovpålagt forankring

### Beskrivelse av sperremekanisme

## Pasientens konfidensialitetsrettigheter, logging og logghåndtering

### Beskrivelse av etablert løsning for logging

### Oppbevaring og forvaltning av logger

### Tilgangskontroll av logger

# Risikovurdering

Kapittel 4 inneholder en oppsummering av identifiserte avvik knyttet til etterlevelse av Sikkerhetsprinsipper og -krav for IKT, samt eventuelt foretaksspesifikke krav. Videre beskrives mulige sårbarheter og tilhørende trusselscenarier, og vurdering av risikoens alvorlighetsgrad.

## Krav til løsningen og etterlevelse

### Etterlevelse av sikkerhetsprinsipper og -krav for IKT

Sikkerhetsprinsipper og -krav for IKT er en sammenstilling av de viktigste og vanligste prinsippene for å oppnå tilfredsstillende informasjonssikkerhet i SIKT og tilknyttede miljøer. Prinsippene er bygget over tid, og har en tett tilknytning til blant annet arkitektur- og løsningsdesignprinsipper som foreligger.

I dette avsnittet oppsummeres identifisert avvik med begrunnelse. Med avvik menes det i denne sammenheng at sikkerhetsprinsipper ikke er etterlevd, eller at det ikke har vært mulig å fremskaffe dokumentasjon som kan bekrefte etterlevelse.

*For fullstendig besvarelse av sjekklistene i «Sikkerhetsprinsipper og -krav for IKT», henvises det til vedlegg A.*

| **Område** | **#** | **Sikkerhetsprinsipp som ikke er etterlevd** | **Begrunnelse for avvik** |
| --- | --- | --- | --- |
|  |  |  |  |

**FORKLARING TIL TABELL:**

|  |  |
| --- | --- |
| Område | Angivelse av hvilket område iht. dokumentet «Sikkerhetsprinsipper og -krav for IKT» et avvik tilhører. Eksempler på områder er anskaffelser, databehandling, brukerkontoer, administratorkontoer osv. |
| # (nummer) | Angivelse av nummer på sikkerhetsprinsipp iht. oppsett i dokumentet «Sikkerhetsprinsipper og –krav for IKT» (dokumentreferanse 3) |
| Sikkerhetsprinsipp som ikke er etterlevd | Tekstlig gjengivelse av sikkerhetsprinsipp som ikke er etterlevd. For sikkerhetsprinsipper som ikke er etterlevd er det krysset av «Nei» i sjekklisten (ref. vedlegg A). |
| Begrunnelse for avvik | Skriftlig begrunnelse av hvorfor sikkerhetsprinsippet er vurdert ikke etterlevd. |

### Etterlevelse av foretaksspesifikke krav

## Mulige sårbarheter og tilhørende trusselscenarier

I tabellen beskrives relevante sårbarheter som er identifisert i risikovurderingen. For hver identifiserte sårbarhet er mulig trusselscenario og konsekvens beskrevet.

| **ID** | **Område** | **Mulig sårbarhet** | **Mulig trusselscenario og hendelse** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |

**FORKLARING TIL TABELL:**

|  |  |
| --- | --- |
| ID | Unik identifikasjon knyttet til den enkelte sårbarhet. |
| Område | Angivelse av hvilket område iht. dokumentet «Sikkerhetsprinsipper og -krav for IKT» identifisert sårbarhet tilhører (ref. vedlegg A). Eksempler på områder er anskaffelser, databehandling, brukerkontoer, administratorkontoer osv. |
| Mulig sårbarhet | Beskrivelse av underliggende sårbarhet som muliggjør/er årsak til risiko. |
| Mulig trusselscenario og hendelse | Beskrivelse av hvordan en sårbarhet/svakhet kan utnyttes og mulig hendelse. Et trusselscenario kan være basert på en eller flere sårbarheter, og en sårbarhet kan danne grunnlag for ett eller flere trusselscenarioer. Hvert trusselscenario skal ha et unikt nummer. |

## Vurdering av risiko

I tabellen angis vurdering av risikoens alvorlighetsgrad. Risiko beregnes som et produkt av sannsynlighet og konsekvens. All risiko lik 6 eller høyere ligger utenfor akseptkriterier. For beskrivelse av metodikk, henvises det til dokumentet «Metode for beregning av sannsynlighet og konsekvens» (dokumentreferanse 2)

| **#** | **Mulig trusselscenario og hendelse** | **Mulig virkning**  **(Konsekvens)** | **K**  **I**  **T**  **S** | **K**  **(1-4)** | **S**  **(1-4)** | **(K x S)**  **(1-16)** | **Begrunnelse**  **Sannsynlighet)** | **Utenfor aksept-kriterier** | **Tiltak**  **nr.** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |

**FORKLARING TIL TABELL:**

|  |  |
| --- | --- |
| # (nummer) | Unikt nummer knyttet til den enkelte mulige trusselscenario og hendelse. |
| Mulig trusselscenario og hendelse | Beskrivelse av hvordan en sårbarhet/svakhet kan utnyttes og mulig hendelse. Et trusselscenario kan være basert på en eller flere sårbarheter, og en sårbarhet kan danne grunnlag for ett eller flere trusselscenarier. Hvert trusselscenario skal ha et unikt nummer. |
| Mulig virkning (Konsekvens) | Skriftlig begrunnelse av vurdert konsekvens dersom hendelsen inntreffer. Vurdering av konsekvens skal knyttes opp mot de fire aspektene konfidensialitet (K), integritet (I), tilgjengelighet (T) og sporbarhet (S). For beskrivelse av vurderingskriterier henvises det til dokumentet «SP IS - Metode for beregning av sannsynlighet og konsekvens» (dokumentreferanse 2). |
| KITS | Angir om hendelsen truer informasjonens Konfidensialitet, Integritet, Tilgjengelighet eller Sporbarhet med henholdsvis bokstavene K, I, T, S. |
| Konsekvens (K) | Fastsatt konsekvens (1-4) i henhold til gjeldende metode for beregning av sannsynlighet og konsekvens (dokumentreferanse 2). |
| Sannsynlighet (S) | Fastsatt sannsynlighet (1-4) i henhold til gjeldende metode for beregning av sannsynlighet og konsekvens (dokumentreferanse 2). |
| K x S | Risiko beregnes som produkt av sannsynlighet og konsekvens. Det benyttes skala fra 1-16, hvor 1 er laveste verdi og 16 er høyeste verdi. *All risiko lik 6 eller høyere ligger utenfor akseptkriteriene*. |
| Begrunnelse (Sannsynlighet) | Skriftlig begrunnelse av vurdert sannsynlighet for at hendelsen skal inntreffe. For beskrivelse av vurderingskriterier henvises det til dokumentet «SP IS - Metode for beregning av sannsynlighet og konsekvens» (dokumentreferanse 2). |
| Utenfor akseptkriteriene | Ja dersom K x S ≥ 6, nei dersom K x S < 6. |
| Tiltaksnummer | Unik nummerering av identifisert tiltak. |

# Anbefalte risikoreduserende tiltak

Kapittel 5 inneholder en beskrivelse av anbefalte risikoreduserende tiltak basert på identifisert risiko. For å behandle risiko, må man vite hvilke tiltak som er mulige. Ett enkelt tiltak kan adressere flere sårbarheter, og en sårbarhet kan kreve flere tiltak. En oversikt over dette er viktig for å vurderer kost/nytte verdi av hvert tiltak. I tabellen beskrives forslag til tiltak, samt anbefalt ansvarlig for behandling av tiltak.

| **Tiltak**  **nr.** | **ID** | **Risiko (1-16)** | **Mulig sårbarhet** | **Beskrivelse av tiltak** | **Anbefalt ansvarlig for behandling av tiltak** |
| --- | --- | --- | --- | --- | --- |
| 1 |  |  |  | 1.1  1.2 |  |
|  |  |  |  |  |  |

**FORKLARING TIL TABELL**

|  |  |
| --- | --- |
| Tiltak nr. | Unik nummerering av identifisert tiltak. |
| ID | Unik identifikasjon knyttet til den enkelte sårbarhet. |
| Risiko (1-16) | Risiko beregnes som produkt av sannsynlighet og konsekvens. Det benyttes skala fra 1-16, hvor 1 er laveste verdi og 16 er høyeste verdi. *All risiko lik 6 eller høyere ligger utenfor akseptkriteriene*. |
| Mulig sårbarhet | Beskrivelse av underliggende sårbarhet som muliggjør/er årsak til risiko. |
| Beskrivelse av tiltak | Beskrivelse av anbefalt risikoreduserende tiltak. Ett enkelt tiltak kan adressere flere sårbarheter, og en sårbarhet kan kreve flere tiltak. |
| Anbefalt ansvarlig for behandling av tiltak | Angivelse av anbefalt ansvarlig for behandling av identifiserte tiltak. For adressering av tiltak, er det primært følgende alternativer som benyttes; Prosjektet, Helseforetaket, Sykehuspartner – infrastruktur/plattform, eller Sykehuspartner – forvaltning. |

## 

# VEDLEGG A: Besvart etterlevelse av Sikkerhetsprinsipper og -krav for IKT

<Husk å sjekke gjeldende versjon av Sikkerhetsprinsipper og –krav IKT>

Det styrende dokumentet «Sikkerhetsprinsipper og –krav for IKT infrastruktur, applikasjoner og behandlingsrettete helseregistre, versjon 1.0» er en sammenstilling av nødvendige prinsipper for å oppnå tilfredsstillende informasjonssikkerhet i Helse Sør-Øst. Prinsippene er bygget over tid, og har en tett knyting til bl.a. arkitektur- og løsningsdesignprinsipper som foreligger.

I dette vedlegget følger en fullstendig besvarelse av sjekklistene i «Sikkerhetsprinsipper og –krav for IKT infrastruktur, applikasjoner og behandlingsrettete helseregistre».

# Helse Sør-Østs sikkerhetsprinsipper

# Anskaffelser

Ved anskaffelser skal virksomheten(e) ivareta at leverandører og utstyr i best mulig grad etterlever sikkerhetsprinsippene beskrevet i dette dokumentet. Beskyttelse av data og personinformasjon er sikret slik det kreves i relevante lover og forskrifter, og hvis det er aktuelt, kontraktsbestemmelser.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sikkerhetsprinsipper ved anskaffelser | | Etterlevd | | |
| JA | NEI | I/R |
| 1.1 | Utforming, drift, bruk og administrasjon av informasjonssystemer samstemmer med aktuelle lov(er), forskrift(er) og kontraktsfestede krav til sikring. |  |  |  |
| 1.2 | Anskaffelsen er i tråd med HSØ sine sikkerhetsprinsipper, inkludert dette dokumentet og øvrige dokumenter i HSØs styringssystem for informasjonssikkerhet. |  |  |  |
| 1.3 | Anskaffelsen/systemet med underliggende komponenter skal supporteres i kontraktsperiodens levetid |  |  |  |

# Behandling av personopplysninger

Med behandling av personopplysninger menes all registrering, prosessering, bruk og lagring som gjennomføres. Det er databehandlingsansvarlig som beslutter formålet med databehandlingen. Sykehuspartner [Sykehuspartner erstattes med annen databehandler dersom relevant] er databehandler og utfører sin del av behandlingen etter avtale med databehandlingsansvarlig.

Personopplysninger skal slettes når formålet med behandlingen er oppfylt og det ikke foreligger oppbevaringskrav i annet regelverk som har forrang i forhold til slettekravet av personopplysningsloven. Sletting involverer en fullstendig sletting av opplysninger, fra alle medier opplysningene er lagret på, inklusive sikkerhetskopier.

Behandling av personopplysninger er forankret i personopplysningsloven § 15.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sikkerhetsprinsipper for databehandling | | Etterlevd | | |
| JA | NEI | I/R |
| 2.1 | Det skal være besluttet og godkjent et formål med databehandlingen |  |  |  |
| 2.2 | Det skal være opprettet og godkjent en tjenesteavtale og tjenestespesifikk databehandleravtale mellom Sykehuspartner [evt. annen databehandler] og databehandlingsansvarlig |  |  |  |
| 2.3 | Det skal være opprettet og godkjent databehandleravtaler med eventuelle underleverandører |  |  |  |

# Brukerkontoer

Med brukerkonto menes en representasjon for en digital identitet. I Virksomheten skal alle ansatte ha en personlig konto. Tilgang til informasjon, informasjonsbehandlingsutstyr og virksomhetsprosesser skal kontrolleres på grunnlag av virksomhetsbehov og sikkerhetsbehov.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Sikkerhetsprinsipper for brukerkontoer | | Etterlevd | | | |
| JA | NEI | | I/R |
| 3.1 | Det skal kun benyttes personlige brukere. Fellesbrukere eller på annen måte deling av brukerkontoer skal ikke forekomme. |  |  | |  |
| 3.2 | Brukerkontoer skal entydig knyttes opp mot den digitale identitet til den enkelte, og ivareta kravene om uavviselighet og sporbarhet ved autentisering. |  |  | |  |
| 3.3 | Brukerkontoer skal deaktiveres etter arbeidsforholdet er opphørt eller behovet for tjenesten bortfaller |  |  | |  |
| 3.4 | Brukerkontoer skal ikke gis administrative rettigheter. For dette formålet skal personlige administratorkontoer opprettes. |  |  | |  |
| 3.5 | Brukerkontoer skal følge instruks for passordsikkerhet |  |  | |  |
| 3.6 | Kravene til passordlengde og -kompleksitet håndheves automatisk av systemet. |  |  | |  |
| 3.7 | Brukere skal hindres i å benytte informasjonsbehandlingsutstyr til ikke-autoriserte formål. |  |  | |  |
| 3.8 | Varigheten av aktive sesjoner skal tidsavgrenses for å forhindre brukerne fra å holde sesjonene åpne slik at ny autentisering kan unngås |  |  | |  |
| 3.9 | Det er gjennomført, eller planlagt gjennomført, en hensiktsmessig opplæring i bevisstgjøring og regelmessig ajourføring i policy og prosedyrer som er relevant for brukere av systemet. Dette gjelder alle brukere og administratorer av systemet, samt eventuelle kontraktører og tredjepartsbrukere. |  |  | |  |
| Spesielt for behandlingsrettede helseregistre  PJL §22 | | Etterlevd | | | |
| JA | | NEI | I/R |
| 3.10 | Arbeidsforholdet[[2]](#footnote-2)[[3]](#footnote-3) til den enkelte skal være entydig identifiserbart så lenge bruker er pålogget og kunne spores i de behandlingsrettede helseregistre den enkelte er gitt tilgang til. |  |  | |  |
| 3.11 | Det skal være mulig å entydig identifisere hvem som er arbeidsgiver til den enkelte ansatte (entydig identitet). Dersom det foreligger flere ansettelsesforhold skal applikasjonen sørge for at det er entydig i hvilket forhold den ansatte til enhver tid opptrer. |  |  | |  |
| 3.12 | Identiteten[[4]](#footnote-4) til den enkelte som bruker ett eller flere behandlings­rettede helseregistre skal være gjennomgående sporbar på tvers av disse. |  |  | |  |
| 3.13 | Autentisering skal støtte identitetsutveksling ved hjelp av SAML forsterket med kryptografisk signering, eller tilsvarende. |  |  | |  |
| 3.14 | Den autoritative kilden for ansattidentiteter skal være det regionale lønns- og personalsystemet |  |  | |  |
| 3.15 | Den autoritative kilden for organisasjonsenheter i spesialisthelse­tjenesten skal være det til enhver tid gjeldende nasjonale helseadministrative register (p.t. Register over Enheter i Spesialisthelsetjenesten[[5]](#footnote-5)) |  |  | |  |

# Personlige administratorkontoer

Personlige administratorkontoer skal benyttes for å oppnå eller utføre administrative oppgaver. Administratorkontoene er knyttet til den ansattes digitale identitet.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sikkerhetsprinsipper for personlige administratorkontoer | | Etterlevd | | |
| JA | NEI | I/R |
| 4.1 | Administratorkontoer skal knyttes opp mot en digital identitet, slik at kravet om uavviselighet og sporbarhet ivaretas. |  |  |  |
| 4.2 | Administratorkontoer skal følge instruks for passordsikkerhet |  |  |  |
| 4.3 | Kravene til passordlengde og -kompleksitet håndheves automatisk av systemet. |  |  |  |
| 4.4 | Administratortilgang skal begrenses iht. dokumentert behov |  |  |  |
| 4.5 | Administratorkontoer skal deaktiveres når behovet bortfaller |  |  |  |

# Upersonlige system- og administratorkontoer

Med upersonlige system- og administratorkontoer menes kontoer som ikke er knyttet til person, dvs. kontoer som ”root”, ”db\_admin”, ”administrator” og så videre, samt også servicekontoer. Tilgang til disse skal begrenses.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sikkerhetsprinsipper for upersonlige system- og administrasjonskontoer | | Etterlevd | | |
| JA | NEI | I/R |
| 5.1 | System- og administratorbrukere skal opprettes med unike passord, og passordet skal ha høy kompleksitet, i tråd med instruks om passord |  |  |  |
| 5.2 | System- og administratorpassord skal inngå i virksomhetens passordhvelv. |  |  |  |

# Autentisering

Med autentisering menes som regel verifisering av en brukerkonto gjennom passord eller andre mekanismer. En digital identitet kan ha flere brukerkontoer, og tilgang til informasjonssystemer styres som hovedregel gjennom autentiseringen av en brukerkontos passord.

Pasientjournalloven §22 angir at det skal være tilgangs­styring, log­ging og etterføl­gende kontroll.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Sikkerhetsprinsipper for autentisering | | | | Etterlevd | | | | |
| JA | | NEI | I/R | |
| 6.1 | | Autentisering skal gjøres mot sentral autentiseringsløsning | |  | |  |  | |
| 6.2 | | Passord skal transporteres kryptert etter gjeldende policy i Helse Sør-Øst. | |  | |  |  | |
| 6.3 | | Passord skal lagres som hash etter gjeldende policy i Helse Sør-Øst. | |  | |  |  | |
| 6.4 | | Systemet skal kunne håndheve vedtatt instruks for passordkompleksitet | |  | |  |  | |
| 6.5 | | Passord er personlige og skal ikke deles | |  | |  |  | |
| 6.6 | | Passord skal aldri oppbevares skriftlig, annet enn i godkjent hvelv | |  | |  |  | |
| 6.7 | | Passord skal ikke benyttes i klartekst ved bruk av maskinelle rutiner, f.eks. i script. | |  | |  |  | |
| 6.8 | | Autentiseringen må ha tilstrekkelig styrke ihht gjeldende retningslinjer.  Styrken på autentiseringen avgjøres av anbefalingen fra en risikovurdering av tjenesten. Nasjonale føringer legges til grunn [[6]](#footnote-6). | |  | |  |  | |
| 6.9 | | Det skal benyttes to-faktorautentisering, hvorav passord er en av faktorene ved:   * Tilgang fra eksterne nettverk (ekstranett, Internett, leverandører) * Tilgang fra klientnettverket mot admin nettverket   Styrken på autentiseringen avgjøres av anbefalingen fra en risikovurdering av tjenesten. Nasjonale føringer legges til grunn[[7]](#footnote-7). | |  | |  |  | |
| 6.10 | | Passordhvelv skal benyttes for alle ikke-personlige kontoer, for eksempel servicekontoer eller administratorbrukere | |  | |  |  | |
| 6.11 | | Alle tilgangsforespørsler til integrasjonsgrensesnitt skal autentiseres vha en internasjonal standard tilsvarende Security Assertion Markup Language[[8]](#footnote-8) | |  | |  |  | |
| 6.12 | | Informasjonssystemer skal støtte Single Sign-On (SSO) | |  | |  |  | |
| 6.13 | Ansatte i andre virksomheter skal kunne automatisk autentiseres vha en internasjonal standard og protokoll for sikker utveksling av identiteter mellom ulike organisasjoner tilsvarende SAML (Security Assertion Markup Language) | |  | |  | | |  |

# Autorisering

Med autorisering menes å gi korrekte tilganger til en autentisert konto. I Virksomheten er det som hovedregel katalogtjenesten *Active Directory* som er autoritativ for rettigheter og tilganger.

Det settes en rekke krav til tilgangskontroll for regionale journalsystemer og registre. Pasientjournalloven §22 sier at “det skal gjennom planlagte og systematiske tiltak sørges for tilfredsstillende informasjons­sikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet”. “Dette omfatter blant annet å sørge for tilgangsstyring, logging og etterfølgende kontroll”.

Pasientjournalloven åpner for nye måter å organisere pasientjournaler og tilganger til slike journaler. Loven endrer imidlertid ikke på kravet og forutsetningen om at det kun skal gis tilgang til opplysninger som er nødvendige og relevante for å yte helsehjelp, og rammene for helsepersonells taushetsplikt er ikke endret i forhold til den tidligere lovgivningen. Dette følger av alminnelige regler om taushetsplikt for helsepersonell, og forutsetningen er presisert i blant annet pasientjournalloven § 6, § 7 og i § 19. Dette innebærer at løsninger med felles behandlingsrettede helseregistre må kunne ivareta de grunnleggende kravene knyttet til konfidensialitet om pasientenes helseopplysninger.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sikkerhetsprinsipper for autorisering | | Etterlevd | | | | |
| JA | NEI | | I/R | |
| 7.1 | Tilganger skal være basert på rollestyring |  |  | |  | |
| 7.2 | Tilganger skal være på et lavest mulig nivå |  |  | |  | |
| 7.3 | Tilganger skal være tidsbegrenset for innleid personell, og skal ikke overskride innleieavtalens varighet |  |  | |  | |
| 7.4 | Tilganger skal fjernes når formålet opphører |  |  | |  | |
| 7.5 | Tilganger skal loggføres, endringer i tilganger og hvem som beslutter endringer i tilganger skal loggføres |  |  | |  | |
| Spesielt for behandlingsrettede helseregistre  PJL §22  POL§13  POF §§ 2-1, 2-11, 2-12, 2-13, 2-14 | | Etterlevd | | | | |
| JA | | NEI | | I/R |
| 7.6 | Behandlingsrettede helseregistre skal støtte attributtbasert tilgangskontroll der attributtene som benyttes til autorisasjon (tilgangskontroll) minimum omfatter ansettelses- eller arbeidsforholdet til brukeren og rollen [[9]](#footnote-9)brukeren har i sitt påloggede arbeidsforhold. |  | |  | |  |
| 7.7 | Rollen [[10]](#footnote-10) brukeren har i et behandlingsrettet helseregister skal avgjøre hvilken tilgang brukeren får til informasjonen og applikasjonsfunksjonene i det behandlingsrettede registeret |  | |  | |  |
| 7.8 | Attributtene som følger med identiteten til den ansatte/innleide ved pålogging til et behandlingsrettet helseregister, skal i tillegg kunne avgjøre hvilke tilganger den ansatte har til funksjonene i det behandlingsrettede helseregisteret |  | |  | |  |
| 7.9 | Rollen [[11]](#footnote-11)den ansatte innehar i et behandlingsrettet helseregister skal skille dennes tilganger begrenset i forhold til pasienter i aktiv behandling [[12]](#footnote-12)på angitte organisasjonsenheter, samt tid i forkant og etterkant av aktiv behandling |  | |  | |  |
| 7.10 | Rollen den ansatte innehar i et behandlingsrettet helseregister skal gi mulighet for den ansatte selv til å beslutte tilgang til ikke-aktive[[13]](#footnote-13) pasienter |  | |  | |  |
| 7.11 | Rollen den ansatte innehar i et behandlingsrettet helseregister skal gi mulighet for den ansatte til å beslutte tilgang for en kollega som selv ikke har tilgang til pasienten som ikke er under aktiv behandling |  | |  | |  |
| 7.12 | Rollen den ansatte innehar i et behandlingsrettet helseregister skal gi mulighet for tilgang til pasienter via «arbeidsgruppe» (postliste) (organi­sering og gruppering av pasienter uten avhengighet til organisa­sjonens formelle enheter) |  | |  | |  |
| 7.13 | Rollen den ansatte innehar i et behandlingsrettet helseregister skal gi mulighet for å eksplisitt beslutte tilgangen til pasienter begrenset til (skal kunne velge en eller flere kriterier samtidig):   1. hvilke sett av organisasjonsenheter pasienten tidligere har vært behandlet ved innen et foretak, eller hele foretaket under ett 2. hvilke sett av organisasjonsenheter pasienten tidligere har vært behandlet ved på tvers av flere foretak, eller inkludert et eller flere hele foretaket 3. gitte diagnoser/kombinasjoner av diagnoser, eller alle diagnoser 4. antall måneder/år tilbake i tid for når pasienten ble behandlet av gitt org.enhet 5. inkluder døde pasienter ja/nei 6. pasienter i et gitt pasientforløp |  | |  | |  |
| 7.14 | Rollen den ansatte innehar i et behandlingsrettet helseregister skal gi mulighet for å delegere pasienter til en eksisterende arbeidsgruppe ut fra følgende utvalgskriterier:   1. pasienter som har vært behandlet ved gitte sett av organisasjonsenheter innen et foretak, eller hele foretaket under ett 2. pasienten som har vært behandlet ved gitte sett av organisasjonsenheter på tvers av flere foretak, eller et eller flere foretaket 3. pasienter med valgt kombinasjon(er) av diagnose- og prosedyrekoder, eller alle diagnoser 4. antall måneder/år tilbake i tid for når pasienten ble behandlet av gitt org.enhet 5. inkluder døde pasienter ja/nei 6. pasienter i et gitt pasientforløp |  | |  | |  |
| 7.15 | Det skal være mulig å entydige identifisere hvem som er juridisk[[14]](#footnote-14)- og/eller medisinsk ansvarlig [[15]](#footnote-15)for en gitt pasienten innen en juridisk enhet og på tvers av juridiske enheter involvert i pasientens behandling |  | |  | |  |

# IAM og Identitetsforvaltning

Dette kapittelet gjelder kravstilling til applikasjoner som skal benytte IAM (Identity and Access Management – Identitets- og tilgangsstyring).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sikkerhetsprinsipper for IAM | | Etterlevd | | |
| JA | NEI | I/R |
| 8.1 | Applikasjonen må støtte federering som autentiseringsmekanisme |  |  |  |
| 8.2 | Applikasjonen må støtte anerkjente federeringsteknologistandarder (f.eks. SAML 2.0 eller OpenID Connect) som autentiseringsmekanisme. |  |  |  |
| 8.3 | Ved bruk av SAML bør applikasjonen støtte "Service Provider initiated" federeringsprosess. |  |  |  |
| 8.4 | Ved pålogging til kliniske applikasjoner må som minimum attributtene brukerid, organisasjonstilknytning og rolle tas imot og behandles for å etablere sikkerhetssesjon. |  |  |  |
| 8.5 | Applikasjonen må håndheve sikkerhetssesjonen. Dette inkluderer, men er ikke begrenset til inaktivitet, start- og sluttidspunkt på token. |  |  |  |
| 8.6 | Ved behov for ny eksplisitt autentisering (reautentisering og/eller autentisering av annen bruker) i en allerede etablert sikkerhetssesjon bør applikasjonens federeringfunksjon benyttes. |  |  |  |
| 8.7 | Applikasjonen bør ha mulighet til å falle tilbake til alternativ autentiseringsmekanisme dersom federeringsløsning er deaktivert eller utilgjengelig. |  |  |  |
| 8.8 | Ved vellykket autentisering av en bruker som ikke er autorisert til å benytte applikasjonen, skal applikasjonen ikke falle tilbake til alternativ autentiseringsmekanisme.Sluttbruker får beskjed om nektet adgang. |  |  |  |
| 8.9 | Tilgang til funksjonalitet og pasientdata i applikasjonen må baseres på kombinasjon av brukers rolle og organisasjonstilknytning. I hovedsak gir rolle tilgang til funksjoner mens organisasjon styrer pasienttilgang. Dette støttes ved bruk av interne tilgangskontrollmekanismer og/eller ekstern autoriseringstjeneste. |  |  |  |
| 8.10 | Applikasjonen bør spørre ekstern autoriseringstjeneste om det finnes en aktiv pasient-behandlerrelasjon dersom intern tilgangskontrollmekanisme ikke kan avgjøre tilgang. |  |  |  |
| 8.11 | Dersom ekstern autoriseringstjeneste benyttes må kall mot denne gjøres iht internasjonale autoriseringsstandarder som f.eks. XACML og OAuth |  |  |  |
| 8.12 | Applikasjonen må være i stand til å tilpasse seg Helse Sør-Østs sikkerhetsarkitektur relatert til attributtbasert tilgangskontroll (ABAC) |  |  |  |
| 8.13 | Ved nektet tilgang bør applikasjonen presentere begrunnelsen på en forståelig måte til sluttbruker. |  |  |  |
| 8.14 | Applikasjonen må støtte én entydig regional bruker-ID per person (identitet) |  |  |  |
| 8.15 | Applikasjonen bør støtte gruppering av rettigheter ved at roller for tilgang kan defineres og gis rettigheter slik at brukere kan tildeles roller i stedet for individuelle rettigheter |  |  |  |
| 8.16 | Applikasjonen må støtte at det kan være flere roller og/eller organisasjoner knyttet til samme entydige bruker-ID |  |  |  |
| 8.17 | Applikasjonen må støtte unik identifikator for entydig identifikasjon av organisasjonsenheter. |  |  |  |
| 8.18 | Leverandøren må tilpasse sitt produkt slik at tilganger kan differensieres på hvor den ansatte jobber til enhver tid |  |  |  |
| 8.19 | Applikasjonen må støtte provisjonering (oppretting, lesing, endring og sletting) via standardisert programmeringsgrensesnitt (API). Programmeringsgrensesnittet må:  - Være godt nok dokumentert til at en erfaren utvikler kan benytte grensesnittet uten opplæring  - Ha standardisert autentiseringsmekanisme  - Benytte kryptert kommunikasjon  - Kommunisere over HTTP, LDAP eller SQL  Programmeringsgrensesnittet bør:  - Være REST-API over HTTPS tilnærmet SCIM-standarden |  |  |  |
| 8.20 | APIet må muliggjøre provisjonering av påloggingsklare brukere med forhåndsdefinerte standardtilganger uten behov for manuelle tilleggsoperasjoner |  |  |  |
| 8.21 | APIet bør muliggjøre tildeling av individuelle rettigheter i tillegg til standardtilganger |  |  |  |
| 8.22 | Applikasjonen bør tilby et brukergrensesnitt for brukeradministrasjon, i tillegg til APIet |  |  |  |
| 8.23 | APIet må muliggjøre uthenting av eksisterende data knyttet til bruker, rolle, organisasjon og tilganger fra applikasjonen |  |  |  |

# Sperring (Pasientens konfidensialitetsrettigheter)

Den enkelte pasient skal kunne motsette seg at helseopplysninger blir brukt i den videre behandling av pasienten. Dette refereres oftest til som "rett til sperring". Behandlingsrettede helseregistre må dermed ha støtte for å sperre tilgang til helseopplysninger for en valgt pasient.

Pasientjournalloven § 7 litera c angir at ”Behandlingsrettede helseregistre skal være utformet og organisert slik at krav fastsatt i eller i medhold av lov kan oppfylles. Dette gjelder blant annet regler om» «c) retten til å mot­sette seg behand­ling av helseopplysninger, jf. § 17”

Pasientjournalloven § 17 angir ”Pasienten eller brukeren kan motsette seg at a) helseopp­lysninger i et behand­lings­rettet helseregister med hjemmel i §§ 8 til 10 gjøres tilgjengelig for helsepersonell etter § 19, jfr. helsepersonel­loven §§ 25 og 45 og pasient- og brukerrettighets­loven § 5-3.”

Manuell støtte i forkant for sperring:

1. Journalansvarlig[[16]](#footnote-16) skal forklare pasienten konsekvensen ved sperring, og at det eventuelt kan ha betydning for videre helsehjelp. Dersom pasienten er samtykkekompetent, og har fått forklart konsekvensene, skal pasientens krav om sperring etterkommes
2. Dersom ikke kravet etterkommes, skal det sendes informasjon til pasienten om retten til å klage til helsetilsynet i fylket

Behandlingsrettede helseregistre må derfor understøtte at pasienten kan detaljere hvem som ikke skal kunne ha tilgang i sin journal og hva det /hvilken informasjon det skal begrenses innsyn i.

Tabellen under angir kravene til slik sperring. Kravene gjelder både internt i et helseforetak og mellom helseforetak. Kravene skal anvendes både på eksisterende informasjon og dokumenter og framtidig informasjon og dokumenter som skal etableres.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Spesielt for behandlingsrettede helseregistre  PJL §§7c og 17 | | Etterlevd | | | | |
| JA | | NEI | | I/R |
| 9.1 | Det skal være mulig i et behandlingsrettet helseregister og etter forespørsel fra en pasient, å kunne begrense tilgangen til journalen til en pasient, slik at en **navngitt person**, eksempelvis nabo eller nær slektning eller andre entydige identifiserbare personer, **ikke** **skal ha tilgang** til hele eller utvalgte deler av journalen til pasienten |  |  | |  | |
| 9.2 | Det skal være mulig i et behandlingsrettet helseregister og etter forespørsel fra en pasient, å kunne begrense tilgangen til journalen til en pasient, slik at utelukkende (alle) **enkeltpersoner eller enkeltpersoner i en gitt rolle**, eksempelvis alle leger, **skal ha tilgang** til journalen til pasienten, og dermed sperre tilgangen for alle andre |  |  | |  | |
| 9.3 | Det skal være mulig i et behandlingsrettet helseregister og etter forespørsel fra en pasient, å kunne begrense tilgangen til journalen til en pasient, slik at **kun** **ansatte** som tilhører en eller flere **organisasjonsenheter**, eksempelvis avdeling på et lokalsykehus, **skal ha tilgang** til journalen til pasienten, og dermed sperre tilgangen for alle andre brukerne |  |  | |  | |
| 9.4 | Kriteriene i krav 9.2 og 9.3 (de to foregående kravene) skal kunne kombineres for å definere hvem som skal gis tilgang til journalen til en pasient, og dermed sperre tilgang for alle andre |  |  | |  | |
| 9.5 | Det skal være mulig i et behandlingsrettet helseregister og etter forespørsel fra en pasient, å kunne begrense tilgangen til journalen til en pasient, slik at alle **enkeltpersoner eller enkeltpersoner i en gitt rolle**, eksempelvis sykepleier eller fysioterapeut, **ikke skal ha tilgang** til journalen til pasienten, og dermed sperre tilgangen for disse brukerne |  |  | |  | |
| 9.6 | Det skal være mulig i et behandlingsrettet helseregister og etter forespørsel fra en pasient, å kunne begrense tilgangen tiljournalen til en pasient, slik at **ansatte** tilhørende en eller flere **organisasjonsenheter**, eksempelvis en avdeling, lokalsykehus eller foretak, **ikke** **skal ha tilgang** til journalen til pasienten, og dermed sperre tilgangen for disse brukerne |  |  | |  | |
| 9.7 | Kriteriene i krav 9.5 og 9.6 (de to foregående kravene) skal kunne kombineres for å definere hvem som ikke skal gis tilgang til journalen til en pasient |  |  | |  | |
| 9.8 | Det skal være mulig i et behandlingsrettet helseregister og etter forespørsel fra en pasient, å kunne **sperre tilgangen for en definert periode, inkludert på ubestemt tid fremover,** til enkelt **dokumenter** i journalen til en pasient. Kravet må kunne gjennomføres på dokumenter sperret etter alle kriteriene angitt, ref kravsettene angitt under 9.1-9.7 |  |  | |  | |
| 9.9 | Det skal være mulig i et behandlingsrettet helseregister og etter forespørsel fra en pasient, å kunne sperre **tilgangen for en definert periode, inkludert på ubestemt tid fremover,** til enkelte **dokumenttyper** som vil bli opprettet i journalen til en pasient. Kravet må kunne gjennomføres på dokumenter sperret etter alle kriteriene angitt, ref. kravsettene angitt under 9.1-9.7 |  |  | |  | |
| 9.10 | Det skal være mulig i et behandlingsrettet helseregister og etter forespørsel fra en pasient, å kunne sperre tilgangen for **alle dokumenter** som er opprettet i en definert periode i journalen til en pasient |  |  | |  | |
| 9.11 | Det skal være mulig i et behandlingsrettet helseregister og etter forespørsel fra en pasient, å kunne kun **gi tilgangen for alle dokumenter** som er opprettet i en definert periode i journalen til en pasient |  |  | |  | |

# Ikke-benekt (Digital signering med sertifikat)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Spesielt for behandlingsrettede helseregistre | | Etterlevd | | | | |
| JA | | NEI | | I/R |
| 10.1 | Avsender skal kunne digitalt signere utvalgte dokumenter med kvalifisert sertifikat |  |  | |  | |

# Sporbarhet

Med sporbarhet menes å kunne bevare nødvendige detaljer knyttet til en handling. Under begrepet sporbarhet ligger også begrepet uavviselighet, som er å bekrefte at en handling eller et informasjonselement er uendret, og at det entydig kan knyttes til en bestemt digital identitet. Uavviselighet er i mange sammenhenger også omtalt som ikke-benekting. Uavviselighet benyttes også i sammenheng med autorisering og autentisering.

Pasientjournalloven §22 angir at det skal være tilgangs­styring, log­ging og etterføl­gende kontroll. Bruk av informasjonssystem skal dokumenteres. Dette følger av pasientjournalloven § 22, jf. personopplysningsforskriften § 2-8 og § 2-14. Det stilles videre krav om at loggene skal kontrolleres.

Pasientjournalloven §18 angir at “pasienten eller brukeren har rett til informasjon og innsyn i behandlingsrettede helseregistre etter pasient- og brukerrettighetsloven § 5-1, helsepersonelloven § 41 og personopplysningsloven § 18 flg. Dette omfatter også innsyn i hvem som har hatt tilgang til eller fått utlevert helseopplysninger som er knyttet til pasientens eller brukerens navn eller fødselsnummer.”

Behandlingsrettede helseregistre må derfor understøtte krav om sporbart på hvem som har fått tilgang til eller utlevert helseopplysninger.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sikkerhetsprinsipper for sporbarhet | | Etterlevd | | | | |
| JA | NEI | | I/R | |
| 11.1 | Alle relevante handlinger skal logges. Relevante handlinger skal måles opp mot informasjonssystemet, men som et minimum skal følgende logges:   * Alle typer innlogginger, inkl. forsøk på innlogginger * Oppretting, endring og sletting av informasjonsobjekter * Oppretting, endring og sletting av andre brukere * Innsyn eller endring i helseopplysninger * Endringer, eller forsøk på endringer, i systemkonfigurasjonen |  |  | |  | |
| 11.2 | Endringer i en tjeneste skal dokumenteres i systemdokumentasjonen, og endringer som påvirker informasjonssikkerheten skal risikovurderes |  |  | |  | |
| 11.3 | Logging skal legge til rette for at helseforetakene kan avdekke sikkerhetsbrudd og forsøk på misbruk skal kunne oppdages |  |  | |  | |
| 11.4 | Logger skal tilgangsstyres slikt at de beskyttes mot manipulering/endring |  |  | |  | |
| 11.5 | Logger skal ha tidsstempling og være synkronisert mot sentral NTP-server |  |  | |  | |
| 11.6 | Logger som er relevante for informasjonssikkerheten skal kunne overføres til sentralt loggmottak |  |  | |  | |
| 11.7 | Logger skal gjennomgås manuelt eller automatisk basert på forhåndsdefinerte kriterier. |  |  | |  | |
| 11.8 | Logger skal oppbevares i tråd med krav. Som minimum gjelder 6 måneders lagring for sikkerhetslogger, lagring utover dette må spesifiseres i avtale. For pasientjournallogger eller andre logger knyttet til behandlingsrettede registre, gjelder egne krav. |  |  | |  | |
| Spesielt for behandlingsrettede helseregistre  PJL §§ 18, 22 og 23  POL §§13, 14, 16 og18f  POF §§ 2-4, 2-5, 2-11, 2-14 og 2-16 | | Etterlevd | | | | |
| JA | | NEI | | I/R |
| 11.9 | All ***definert aktivitet*** i behandlingsrettede helseregistre skal loggføres dog ikke være begrenset til følgende funksjoner/aktiviteter:   1. pålogging 2. utlogging 3. åpning av pasientjournal 4. lesing i pasientjournal 5. skriving i pasientjournal 6. «sletting» av pasientjournal 7. sperring av pasientjournal 8. fletting 9. utskrift 10. oppretting og endring av tilganger og rettigheter 11. kopiering og sletting av brukerroller 12. eksport av datasett 13. søk som er gjort |  |  | |  | |
| 11.10 | Følgende informasjon skal minimum lagres ved tilgang og aktivitet i et behandlingsrettet helseregister:   * 1. Bruker, og hvilken av brukerens roller som var aktiv, som har forsøkt utført eller gjennomført tilgang/enhver form for aktivitet   2. Dataelement endret   3. Om dataelement endret er opprettet, lest, endret, skrevet ut, slettet eller annen aktivitet som det er mulig for autoriserte å gjennomføre   4. Tidspunkt for gjennomføring/hendelsen   5. Angivelse av enhet hvor aktivitet/uautorisert tilgang er forsøkt utført og evt. gjennomført |  |  | |  | |
| 11.11 | Det skal være mulig **manuelt** og **automatisert** å hente ut **loggdata** fra behandlingsrettede helseregistre |  |  | |  | |
| 11.12 | Tjenestekonsumenter fra andre juridiske enheter som bruker delsystemene i løsningen, skal kunne spores i regional klinisk løsning, samt i den plattformen og de infrastrukturtjenester som utgjør sikkerhetsarkitekturen |  |  | |  | |

# Serversikkerhet

Med serversikkerhet menes de tiltakene som er implementert for å oppnå akseptabel risiko for servere.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sikkerhetsprinsipper for serversikkerhet | | Etterlevd | | |
| JA | NEI | I/R |
| 12.1 | Serveren skal som minimum herdes i tråd med instruks fra Sykehuspartner. Ved konflikt i kravsett mellom applikasjonsleverandør og Sykehuspartner, skal det gjennomføres risikovurdering |  |  |  |
| 12.2 | Serveren skal ha installert gjeldende sikkerhetsoppdateringer og antivirussignaturer innen rimelig tid iht. kritikalitet. |  |  |  |
| 12.3 | Serveren skal inngå i driftsovervåkingen. |  |  |  |
| 12.4 | Servere skal ha identifiserte krav for:   * Back-up * Forsvarlig patching * Tilgjengelighet, inkludert: * Feilrettingstid * Redundans og GEO redundans |  |  |  |
| 12.5 | Serveren skal synkronisere klokken mot sentral NTP-server |  |  |  |
| 12.6 | Serveren skal avgi logger til sentralt loggmottak |  |  |  |
| 12.7 | Bruk av ressurser skal inn i regime for overvåking og justering, og det bør foretas beregninger over framtidige kapasitetsbehov for å sikre at systemet oppnår påkrevd ytelse |  |  |  |

# Klientsikkerhet

Med klientsikkerhet menes de tiltakene som er implementert for å oppnå akseptabel risiko for klienter.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sikkerhetsprinsipper for klientsikkerhet | | Etterlevd | | |
| JA | NEI | I/R |
| 13.1 | Klienter skal ha kryptert harddisk |  |  |  |
| 13.2 | Klienter skal ha automatisk installasjon av sikkerhetsoppdateringer og antivirussignaturer |  |  |  |
| 13.3 | Klienter skal ha automatisk låsing av skjerm m/ passord |  |  |  |
| 13.4 | Klienter skal være innkjøpt, forvaltet, konfigurert og godkjent av Virksomheten. Klienter som ikke eies av Virksomheten kan heller ikke kobles til Virksomhetens nettverk[[17]](#footnote-17) uten at det foreligger en godkjent risikovurdering. |  |  |  |
| 13.5 | Brukere skal ikke ha administrasjonsprivilegier på egen klient. Brukere skal ikke kunne deaktivere lokale sikkerhetskontroller |  |  |  |
| 13.6 | Klienter skal avlevere relevante logger til sentralt loggmottak |  |  |  |
| 13.7 | Klienter skal kun ha godkjent programvare installert |  |  |  |
| 13.8 | Klienter skal alltid benytte VPN når man er utenfor Virksomhetens infrastruktur, for eksempel private eller offentlige nettverk |  |  |  |
| 13.9 | Klienter skal autentiseres gjennom klientsertifikater for å kunne koble seg på Virksomhetens nettverk. |  |  |  |

# Applikasjonssikkerhet

Med applikasjonssikkerhet menes sikkerhet i de tjenestene som benyttes for å utføre databehandlingen.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sikkerhetsprinsipper for applikasjonssikkerhet | | Etterlevd | | |
| JA | NEI | I/R |
| 14.1 | Applikasjonen skal ha egen tilgangskontroll, med autentisering og autorisering mot sentral tjeneste |  |  |  |
| 14.2 | Applikasjonen skal avgi relevante sikkerhetslogger til sentralt loggmottak |  |  |  |
| 14.4 | Applikasjonen skal styres gjennom Virksomhetens applikasjonsforvaltning |  |  |  |
| 14.5 | Det skal legges til rette for effektiv og hurtig installasjon av sikkerhetsoppdateringer. Om nødvendig skal det opprettes eget testmiljø for å verifisere oppdateringene |  |  |  |
| 14.6 | Applikasjonen skal benytte en trelagsarkitektur for å begrense eksponering av bakenforliggende database |  |  |  |
| 14.7 | Applikasjonen skal kryptere data som går i transitt utenfor vår fysiske kontroll |  |  |  |

# Administrasjon

Med administrasjon menes den driftsoppgaven som må utføres for at IKT-utstyr og tjenester skal fungere i tråd med hensikt og formål.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sikkerhetsprinsipper for administrasjon | | Etterlevd | | |
| JA | NEI | I/R |
| 15.1 | Administrasjon av virksomhetens servere og tjenester skal gjøres gjennom et eget administrasjonsnettverk |  |  |  |
| 15.2 | Administrasjon av virksomhetens servere og tjenester skal gjøres av autorisert personell, med tilhørende personlige administratorbrukere |  |  |  |
| 15.3 | Det skal benyttes to-faktorautentisering for å koble til administrasjonsnettverket |  |  |  |
| 15.4 | Administrasjonsnettverket skal ikke ha tilgang til Internett eller andre eksterne nettverk |  |  |  |
| 15.5 | Servere i administrasjonsnettverket skal sikkerhetsoppdateres på lik linje som vanlig produksjonsutstyr |  |  |  |
| 15.6 | Servere i administrasjonsnettverket skal avgi logger til sentralt loggmottak på lik linje som vanlig produksjonsutstyr |  |  |  |
| 15.7 | Utveksling av informasjon og programvare mellom virksomheter må baseres på en formell utvekslingspolicy, gjennomført i henhold til utvekslingsavtaler, og skal være i samsvar med all relevant  Lovgivning. |  |  |  |

# Avhending

Med avhending menes at IKT-utstyr må skiftes ut. Dette innebærer at IKT-utstyret ikke lenger vil inngå i informasjonsbehandlingen i virksomheten, og skal enten destrueres, resirkuleres, selges, leveres tilbake til leasing leverandør, gis bort eller på annen måte avslutte det juridiske eierskapet hos virksomheten.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sikkerhetsprinsipper for avhending | | Etterlevd | | |
| JA | NEI | I/R |
| 16.1 | Avhending av IKT-utstyr som inneholder helse- eller personopplysninger skal alltid sikres mot uautorisert innsyn.og gjøres slik at innholdet garantert ikke kan gjenskapes |  |  |  |
| 16.2 | Lagringsmedium som inneholder helse- eller personopplysninger, selv om disse er kryptert, skal merkes på en tilstrekkelig måte. |  |  |  |
| 16.3 | Avhending til tredjepart kan ikke gjennomføres før det foreligger godkjent risikovurdering og signert databehandleravtale |  |  |  |

# Leverandører og annet eksternt personell

Med leverandører menes ekstern tredjepart som utfører databehandling, vedlikehold, service, drift, forvaltning eller lignende på vegne av virksomheten.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sikkerhetsprinsipper for leverandører | | Etterlevd | | |
| JA | NEI | I/R |
| 17.1 | Alt innleid personell, samt leverandører som utfører tidsbegrenset arbeid på vegne av virksomheten skal signere taushetserklæring |  |  |  |
| 17.2 | Alle leverandører som utfører databehandling på vegne av helseforetakene i Helse Sør-Øst, eller arbeid hvor innsyn i helse- og personopplysninger er jevnlig forventet å forekomme, skal signere databehandleravtale |  |  |  |
| 17.3 | Alle leverandører som skal behandle helse- og personopplysninger skal kunne dokumentere egen informasjonssikkerhet |  |  |  |
| 17.4 | All leverandørtilgang skal gjøres gjennom Virksomhetens leverandørportal |  |  |  |
| 17.5 | Leverandører kan ikke gis administratortilgang til IKT-utstyr i virksomhetens nettverk, uten at det foreligger en godkjent risikovurdering |  |  |  |
| 17.6 | Leverandører kan ikke flytte eller kopiere data ut fra IKT-utstyr i Virksomhetens nettverk, uten at det foreligger en godkjent risikovurdering |  |  |  |
| 17.7 | Når leverandører gis tilgang skal det etableres tekniske barrierer som hindrer leverandøren i å få tilgang til annet enn hva som er formålet med tilgangen. |  |  |  |

# Datakommunikasjon

Med datakommunikasjon menes flytting eller kopiering av data mellom noder i Helse Sør-Øst sitt nettverk. Det skal etableres **ett** felles fysisk datanettverk for Helse Sør-Øst, som kan segmenteres logisk etter behov. Det er Sykehuspartner som skal etablere og drifte logiske og fysiske nettverk i Helse Sør-Øst. Nye nettverk skal opprettes som en forlengelse av dette felles datanettverket.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sikkerhetsprinsipper for datakommunikasjon | | Etterlevd | | | | |
| JA | | NEI | I/R | |
| 18.1 | Sykehuspartner har ansvar for etablering, drift og kontroll av fysiske og logiske nettverk i Helse Sør-Øst |  | |  |  | |
| 18.2 | Helse Sør-Øst sitt fysiske nettverk skal logisk oppdeles for å understøtte god informasjonssikkerhet |  | |  |  | |
| 18.3 | Løsninger med behov for datakommunikasjon skal støtte mikrosegmentering |  | |  |  | |
| 18.4 | Åpninger mellom logiske nettverk skal kun skje etter risikovurderinger |  | |  |  | |
| 18.5 | Fysiske eller logiske nettverk som ikke kontrolleres av Sykehuspartner, anses å være ekstranettverk. Ekstranett og andre eksterne nettverk skal sammenkobles gjennom Helse Sør-Øst WAN-mottak. Lokale VPN-forbindelser m.v. mot ekstranett eller tredjepart er ikke tillatt |  | |  |  | |
| 16.6 | Alt utstyr som skal bruke SNMP må støtte og konfigureres til å bruke SNMP v3 eller høyere. SNMP skal konfigureres til å bruke autentisering og kryptere trafikken. |  | |  |  | |
| Spesielt for behandlingsrettede helseregistre  POF § 2-11 | | Etterlevd | | | | |
| JA | NEI | | | I/R |
| 18.7 | All datatrafikk mellom endepunktene i et behandlingsrettet helseregister eller mellom behandlingsrettede helseregistre skal være kryptert på applikasjonslaget ihht. Helse Sør-Øst kryptoinstruks. |  |  | |  | |

# Sonemodell

Med sonemodell menes arkitekturbeslutningen hvor Helse Sør-Øst har etablert en sonemodell basert på fire sikkerhetsnivåer.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sikkerhetsprinsipper for sonemodell | | Etterlevd | | |
| JA | NEI | I/R |
| 19.1 | Kommunikasjon skal alltid initieres av tjenesten i det høyeste sikkerhetsnivået |  |  |  |
| 19.2 | Informasjon som går mellom sikkerhetsnivåer skal alltid avidentifiseres/filtreres før informasjonen forlater sitt opprinnelige sikkerhetsnivå |  |  |  |
| 19.3 | Brannmurer skal være lukkede inntil en godkjent risikovurdering gir rom for en endring. Åpninger skal så langt som mulig være i et 1:1-forhold, og for å understøtte dette skal fil-sluser eller lignende benyttes så langt som mulig |  |  |  |
| 19.4 | Informasjon som hentes fra en lavere sikkerhetskontekst skal alltid kontrolleres for ondsinnet kode eller tilsvarende |  |  |  |

# Angrepsflate

Med angrepsflate menes summen av de tjenester og servere som virksomheten eksponerer mot Internett og som dermed utgjør virksomhetens digitale fotspor.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sikkerhetsprinsipper for angrepsflate | | Etterlevd | | |
| JA | NEI | I/R |
| 20.1 | Angrepsflaten skal begrenses til et minimum |  |  |  |
| 20.2 | Alle tjenester som eksponeres eksternt skal penetrasjonstestes, uavhengig av sikkerhetsnivå |  |  |  |
| 20.3 | Alle tjenester som eksponeres eksternt skal plasseres i virksomhetens DMZ |  |  |  |
| 20.4 | Kompromitterte tjenester i DMZ skal ikke kunne benyttes til å gjennomføre angrep mot bakenforliggende systemer |  |  |  |
| 20.5 | En ekstern klient skal aldri kunne sende datapakker inn i systemer bak DMZ. For å oppnå tilstrekkelig informasjonssikkerhet, skal det benyttes fil-sluser hvor trafikkflyten snus |  |  |  |

# Sikker print

Sikker Print er virksomhetens løsning for utskrifter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sikkerhetsprinsipper for Sikker print | | Etterlevd | | |
| JA | NEI | I/R |
| 21.1 | Enheter skal være koblet opp mot Sikker Print løsningen |  |  |  |
| 21.2 | Enheter som kan skrive ut skal stå i et eget VLAN |  |  |  |
| 21.3 | Enheter som bruker Sikker Print skal ha automatisk utlogging etter bruk eller inaktivitet |  |  |  |
| 21.4 | Enheter skal være innkjøpt, forvaltet, konfigurert og godkjent av Virksomheten. Enheter som ikke eies av Virksomheten kan heller ikke kobles til Virksomhetens nettverk uten at det foreligger en godkjent risikovurdering |  |  |  |
| 21.5 | Brukere skal ikke ha administrasjonsprivilegier på utskriftsenheter. Brukere skal ikke kunne deaktivere lokale sikkerhetsfunksjoner på disse enhetene. |  |  |  |

# Dokumentasjon

Virksomheten skal dokumentere informasjonssystemene sine, inkl. konfigurasjon. Dette er forankret i personopplysningsforskriften § 2-16.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sikkerhetsprinsipper for dokumentasjon | | Etterlevd | | |
| JA | NEI | I/R |
| 22.1 | Det er etablert rutiner for bruk av systemet/løsningen |  |  |  |
| 22.2 | Systemdokumentasjon er lagret og holdes oppdatert på godkjent område for oppbevaring i minst fem år etter siste endring |  |  |  |
| 22.3 | Det er opprettet planer for business continuity og disaster recovery for systemet |  |  |  |

# Publikumstjenester

Hvis tjenesten regnes som en publikumstjeneste skal tabellen under fylles ut:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sikkerhetsprinsipper for publikumstjenester | | Etterlevd | | |
| JA | NEI | I/R |
| 23.1 | Publikumstjenester skal settes opp på eget separat nettverk |  |  |  |
| 23.2 | Er Datatilsynets retningslinjer for bruk av [informasjonskapsler](http://www.datatilsynet.no/Teknologi/Internett/cookies/) fulgt? |  |  |  |
| 23.3 | Følger tjenesten lovkravene til [universell utforming](http://www.difi.no/veiledning/universell-utforming-av-ikt) av IKT? |  |  |  |
| 23.4 | Alle eksterne nettsteder driftet av Virksomheten, som har informasjon annet enn kontekst 1 – Åpen, inkludert alle sider som har noen form for pålogging, skal være utstyrt med digitalt sertifikat, og konfigurert for sikker kommunikasjon i henhold til kravene i Virksomhetens krypteringsgspolicy |  |  |  |

# Terminering av eksisterende tjenester

Hvis tjenesten erstatter eller fører til nedstenging av eksisterende tjeneste skal tabellen under fylles ut:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Stenging av eksisterende tjeneste | | Etterlevd | | |
| JA | NEI | I/R |
| 24.1 | Forsvarlig avhending av eksisterende utstyr |  |  |  |
| 24.2 | Lukking av brannmursåpninger |  |  |  |
| 24.3 | Fjerne system- eller administratorkontoer |  |  |  |
| 24.4 | Markere systemet som inaktivt i tjenestekatalogen |  |  |  |

# Annet

Fyll inn annen relevant informasjon om systemet/tjenesten:

|  |
| --- |
|  |

# VEDLEGG B: Andre involvert personer i risikovurderingen

I tabellen under er det oppgitt andre involverte personer i risikovurderingen ut over de som er nevnt i prosjektformalia.

|  |  |
| --- | --- |
| Rolle | Navn |
|  |  |
|  |  |

# VEDLEGG C: Referanser

*Fjern denne teksten: For å sette inn et dokument, sett markøren inn i riktig felt i tabellen, klikk på «SETT INN», gå til menyen over Tekst og velg «Objekt», velg «Opprette fil fra», hent filen ved å klikke «Bla gjennom», og huk av for «Vis som ikon»*

*NB! Saksbehandler er ansvarlig for å sjekke at gyldig versjon av kildehenvisning er vedlagt.*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **#** | **Dokumenteier** | **Dokumentnavn** | **Gyldig fra dato** | **Versjon** | **Dokument** |
| 1 |  |  |  |  |  |
| 2 |  |  |  |  |  |
| 3 |  |  |  |  |  |
| 4 |  |  |  |  |  |

# VEDLEGG D: Helseforetakets behandling

<Dersom dette er en risikovurdering av Regional tjeneste, endres overskrift til Regional behandling>

<Legg ved utfylt vurderingsskjema>

1. Krav regulert i Personopplysningsforskriften §2-4 [↑](#footnote-ref-1)
2. Dette kan løses på ulike måter f.eks. vha en kombinert primærnøkkel som alltid består av en ansatt- og en organisasjonsidentifikator. [↑](#footnote-ref-2)
3. Arbeidsforholdet omfatter både fast- og deltidsansatte, samt innleide og andre som foretaket har ordnet formell instruksjonsrett over for og registrert i HR-systemet (Personalportalen). [↑](#footnote-ref-3)
4. Programvare som krever systemkonti av ulike slag skal ikke ha systemkonti som kan brukes til å få tilgang til innholdet i det behandlingsrettede registeret eller tilgang til å opprette nye brukere i systemet [↑](#footnote-ref-4)
5. Fortiden er RESH den autoritative datakilden for organisasjonsenheter i spesialisthelsetjenesten <https://helsedirektoratet.no/helseadministrative-registre/register-for-enheter-i-spesialisthelsetjenesten-resh> [↑](#footnote-ref-5)
6. <https://www.regjeringen.no/nb/dokument/dep/kmd/lover_regler/retningslinjer/2008/rammeverk-for-autentisering-og-uavviseli/4/id505929/> [↑](#footnote-ref-6)
7. <https://www.regjeringen.no/nb/dokument/dep/kmd/lover_regler/retningslinjer/2008/rammeverk-for-autentisering-og-uavviseli/4/id505929/> [↑](#footnote-ref-7)
8. <https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security> [↑](#footnote-ref-8)
9. Rollen brukeren har er definert i den regionale rollemodellen f.eks. «lege», «sykepleier», «farmasøyt», osv. [↑](#footnote-ref-9)
10. Det forutsettes at den enkelte ansatt/innleide kan ha ulike roller i ulike arbeidsforhold [↑](#footnote-ref-10)
11. Tidsperspektivet må enkelt kunne endres og varieres avhengig av rolle. [↑](#footnote-ref-11)
12. Inneliggende og poliklinikk. [↑](#footnote-ref-12)
13. Pasienter som ikke har noen aktive forhold til foretak [↑](#footnote-ref-13)
14. Med juridisk ansvar menes den organisasjonsenheten som juridisk har ansvaret for pasientens behandling [↑](#footnote-ref-14)
15. Med medisinsk ansvar menes den legen eller psykolog som er pasientansvarlig [↑](#footnote-ref-15)
16. Journalansvarlig: person som omtalt i helsepersonelloven § 39 andre ledd. Journalansvarlig skal være oppnevnt, og har ansvar for innhold av journal, og vil normalt være den som må vurdere krav om retting, sletting og sperring. [↑](#footnote-ref-16)
17. Gjelder ikke gjestenettverk. [↑](#footnote-ref-17)