

A decorative graphic on the left side of the page consisting of a grid of dots. The dots are arranged in a roughly rectangular shape, with the number of dots per row decreasing from bottom to top. Most dots are light blue, but there are several darker blue dots, particularly in the middle section.

Sikkerhetsprinsipper og -krav for IKT- infrastruktur og applikasjoner

1	Hensikt og omfang.....	3
1.1	Behandlingsrettede helseregistre	3
1.2	Hvorfor etablere sikkerhetsprinsipper og -krav?.....	4
1.2.1	Målgruppe.....	4
1.2.2	Hvordan bruke dokumentet	4
1.3	Unntak fra sikkerhetsprinsippene	5
1.4	Forrang over andre dokumenter	5
1.5	Informasjonssystem/tjeneste.....	5
2	Ansvar.....	5
3	Sikkerhetsprinsipper i Helse Sør-Øst	5
3.1	Lover, forskrifter og kontraktbestemmelser.....	6
3.1.1	Databehandling.....	6
3.1.2	Leverandørstyring.....	7
3.1.3	Anskaffelser.....	8
3.2	Tilgangsstyring	9
3.2.1	Identifisering	9
3.2.2	Autentisering.....	9
3.2.3	Autorisering.....	10
3.2.4	Sporbarhet	11
3.2.5	Sperring.....	13
3.3	Teknisk sikkerhet.....	14
3.3.1	Infrastruktursikkerhet	14
3.3.2	Klientsikkerhet.....	14
3.3.3	Serversikkerhet.....	15
3.3.4	Applikasjonssikkerhet.....	16
3.3.5	Sikkerhetskonnfigurasjon av MS SQL-databaser.....	17
3.3.6	Angrepsflate	18
3.3.7	Terminering.....	18
3.4	Forvaltning.....	19
3.4.1	Drift.....	19
3.4.2	Dokumentasjon	20
3.5	Annet.....	20
4	Definisjoner.....	21
5	Avvik eller dissens.....	21
6	Referanser.....	21

Versjonsnummer	Dato	Godkjent av
1.0	22.12.2016	
1.1	23.10.2018	
1.2	18.06.2019	Øyvind Grinde
1.3	21.11.2019	Øyvind Grinde

1 Hensikt og omfang

Sikkerhetsprinsipper og –krav for IKT -infrastruktur og applikasjoner, inkludert behandlingsrettede helseregistre, er en sammenstilling av nødvendige prinsipper og krav for å oppnå tilfredsstillende informasjonssikkerhet i Helse Sør-Øst infrastruktur og porteføljen av applikasjoner. Prinsippene er bygget over tid og har en tett knytning til bl.a. arkitektur- og løsningsdesignprinsipper som også foreligger.

1.1 Behandlingsrettede helseregistre

Pasientjournalloven § 9 og § 19 gir grunnlag (lovhjemmel) for etablering av regionale behandlingsrettede helseregistre (f.eks Medikamentell kreftbehandling, Labdata, PAS/EPJ, Kurve og RIS/PACS) der data kan deles mellom helseforetakene. Pasientjournalloven tillater at det etableres felles behandlingsrettede helseregistre mellom virksomheter (§ 9), og den åpner for å gjøre helseopplysninger tilgjengelige mellom forskjellige virksomheter (§ 19 med forskrift) forutsatt at alle sikkerhetskravene i lov og forskrift er oppfylt. Dette ansvaret tilligger den/evt. de databehandlingsansvarlige.

Dette betyr følgende målrealiseringsmuligheter og føringer for regionale behandlingsrettede registre der pasientjournalen § 9 anvendes:

- Alle pasientdata herunder bestillinger, analyser og svar kan samles i en regional database
- Informasjonen og det medisinske ansvaret i en regional database vil bli tydelig merket, slik at det til enhver tid er enkelt å både gjenfinne informasjonen og det medisinske ansvaret som tilhører det enkelte foretak
- Brukere av det behandlingsrettede helseregisteret og som har nødvendig autorisasjon, skal kunne få tilgang til opplysninger om aktuelle pasienter hentet fra hele databasen i henhold til gjeldende sikkerhetskrav beskrevet i dette dokumentet. Dette vil være personell som behandler pasienten, eller som har (andre) oppgaver som er nødvendig for å kunne behandle den enkelte pasient. Ved pasientbehandling skal pasientforløpet kunne følges gjennom hele den regionale databasen i samsvar med at nødvendig og relevant informasjon skal være tilgjengelig og i samsvar med behov og innen taushetspliktens rammer.
- Brukere av det behandlingsrettede registeret (og) som har foretaksvis administrative oppgaver, skal kunne gis slik begrenset tilgang og kunne gjennomføre oppgaver begrenset til den enkelte juridiske enhets ansvar. Ved administrative oppgaver, inkludert intern kvalitetssikring, skal foretaksgrenser følges. For kvalitetssikring på tvers i hele den regionale databasen, gjelder spesielle krav som det må etableres felles prosedyrer for i regionen. Administrative oppgaver kan kort beskrives som oppgaver som har til formål å administrere helsehjelpen som ytes ved den enkelte behandlingsenhet. Eksempler på administrative oppgaver kan være håndtering av ventelister, innkalling av pasienter, motta avbestillinger og rapportering som grunnlag for finansiering.

Pasientjournalloven er avgrenset til å gjelde all behandling av helseopplysninger som er nødvendig for å yte, administrere og kvalitetssikre helsehjelpen til enkeltpersoner. Pasientjournalloven kan således kun anvendes der formålet med IKT-løsningen er pasientbehandlingen og lagring av helseopplysninger om pasient som benyttes direkte i behandlingen. En konsekvens av dette er at dersom formålet er forskning, vil det behandlingsrettede helseregisteret kunne opptre som datakilde til forskningsregisteret som benyttes, må innfri de gjeldende kravene som stilles av gjeldende lovhomeel for forskningsregisteret.

Sikkerhetskravene spesielt for behandlingsrettede helseregistre er markert. I tillegg vil også andre av sikkerhetskravene være relevante for behandlingsrettede helseregistre, både i grenseflaten mot de behandlingsrettede helseregistre og som infrastruktur. Det er videre ytterligere krav til etablering av felles behandlingsrettede helseregistre, slik som risikovurdering og avtale om felles register. Dette er ikke dekket i dette dokumentet.

Pasientjournalloven setter flere krav og forutsetninger for å kunne realisere regionale behandlingsrettede helseregistre. Med regionale behandlingsrettede helseregistre omfattes der hvor to eller flere foretak har felles register. I tillegg gjelder også Personopplysningsloven med forskrift.

En sentral forutsetning for å gjøre bruk av mulighetsrommet i den nye loven, enten ved tilgang på tvers av juridiske enheter eller i form av en felles journal delt av et eller flere foretak, er at kravene til behandlingsrettet helseregister i pasientjournalloven § 7 er oppfylt. Dette omfatter både krav til teknisk løsning, forutsetninger for forvaltning av identitetshåndtering, systematisk oppfølging av innsynslogg, informasjon til pasient, samt håndtering av rutiner, opplæring og internkontroll, se referanse for relevante dokumenter. Videre må kravene til informasjonssikkerhet være oppfylt. De mest sentrale bestemmelsene i pasientjournalloven for sikkerhetsarkitekturen er §§ 17, 18, 19 og 22. Personopplysningsloven og personopplysningsforskriften gjelder så langt ikke annet følger av pasientjournalloven. Dette dokumentet omfatter de tekniske kravene til løsning, og er (foreløpig) begrenset til mulighetene pasientjournalloven § 9 gir.

Dokumentet beskriver de regionale sikkerhetskravene som er føringer for produkt- og tjenesteleverandører ved anskaffelse og implementering av nye løsninger for behandlingsrettede helseregistre i Helse Sør-Øst. Kravene følger av pasientjournalloven og personopplysningsloven og deres tilhørende forskrifter, samt supplert mht tekniske krav som må delvis ivaretas av applikasjoner og plattform/ infrastruktur.

Sikkerhetskravene tilfredsstilles ved at de enkelte applikasjonene inngår i en regional sikkerhetsarkitektur, som inneholder tjenester som gjør det mulig for applikasjonene å oppfylle kravene i dette dokumentet.

1.2 Hvorfor etablere sikkerhetsprinsipper og –krav?

Sikkerhetsprinsippene og –kravene er en konsekvens av de valgene virksomhetens ledelse har gjort gjennom sikkerhetsmål og sikkerhetsstrategi. Sikkerhetsprinsippene og –kravene er derfor logiske videreføringer og tydeliggjøringer av innholdet i disse.

1.2.1 Målgruppe

Målgruppen for dokumentet er leverandører og tjenesteleverandører, beslutningstakere, informasjonssikkerhetsledere, regionalt sikkerhetsfaglig råd, helseforetakene, programmene og prosjektene i Helse Sør-Øst.

1.2.2 Hvordan bruke dokumentet

Sikkerhetsprinsippene kan brukes som sjekkliste sammen med et løsningsdesign i forbindelse med etablering av tjeneste, endring av tjenester, eller i forbindelse med revisjoner og internkontroll.

Dokumentet brukes også som grunnlag ved anskaffelser av infrastruktur, applikasjoner og tjenester. Deler av kravene er spesifikt rettet mot behandlingsrettede helseregistre, og når dette er relevant så forutsettes det at det gjøres en avklaring av grensesnittet mot eksisterende tjenester og infrastruktur.

Tilgjengeliggjøring av hele dokumentet for leverandøren som bakgrunn, vil kunne være hensiktsmessig. Hvilke krav som leverandøren må besvare og hensynta vil påvirkes av løsning og applikasjoner som skal leveres.

1.3 Unntak fra sikkerhetsprinsippene

Unntak fra sikkerhetsprinsippene skal dokumenteres, legges frem for Regionalt sikkerhetsfaglig råd (RSR) og godkjennes av de helseforetakene som er berørt.

- Prinsippene for forvaltning av regionalt styringssystem for informasjonssikkerhet er omtalt i dokumentet [Overordnede prinsipper for regionalt styringssystem for informasjonssikkerhet](#).

Grunnlaget for å beslutte unntak skal dokumenteres i form av risikovurdering.

1.4 Forrang over andre dokumenter

I tilfelle konflikt med andre styrende dokumenter, må det avklares med informasjonssikkerhetsleder ved berørt foretak hvilket dokument som har forrang. Dette dokumentet er underordnet Helse Sør-Øst sine sikkerhetsmål og sikkerhetsstrategi, og disse dokumentene har ved en evt. konflikt forrang.

1.5 Informasjonssystem/tjeneste

Når dette dokumentet brukes som en del av en tjenesteleveranse skal tabellen under fylles ut:

Navn på informasjonssystem / tjeneste	Systemeier	Tjenesteansvarlig

2 Ansvar

- **Administrerende direktør** er databehandlingsansvarlig for all behandling av helse- og personopplysninger med tilknytning til virksomheten. Administrerende direktør har ansvar for at alle personopplysninger blir behandlet iht gjeldende lovverk, se spesielt helseregisterloven og personopplysningsloven.
- **Ledere** på alle nivåer har ansvar for oppfylling av instruksene i egen enhet.
- **Ansatte og innleide** som i kraft av sin stilling har tilgang til helse- og personopplysninger, inkludert journal, er ansvarlig for å etterleve dette dokumentet.

3 Sikkerhetsprinsipper i Helse Sør-Øst

I dette avsnittet blir det nærmere redegjort for sikkerhetsprinsippene i Helse Sør-Øst. Kapitlet er delt inn i fire hovedavsnitt som gjenspeiler prinsippenes fokusområder. Avsnittene omhandler henholdsvis:

1. Lover, forskrifter og kontraktbestemmelser
2. Tilgangsstyring

3. Teknisk sikkerhet
4. Forvaltning

3.1 Lover, forskrifter og kontraktbestemmelser

Første avsnitt omhandler prinsipper for å sikre at data og helse- og personopplysninger behandles i henhold til relevante lover, forskrifter og kontraktbestemmelser.

Dette avsnittet består av tre underavsnitt: Databehandling, leverandørstyring og anskaffelser.

3.1.1 Databehandling

Med behandling av helse- og personopplysninger menes all registrering, prosessering, bruk og lagring som gjennomføres, herunder tilgang til informasjonssystemer som behandler personopplysninger. Det er databehandlingsansvarlig som beslutter formålet med databehandlingen. Sykehuspartner er databehandler og utfører sin del av behandlingen etter avtale med databehandlingsansvarlig.

Helse- og 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, eksempelvis for journaler. Sletting involverer en fullstendig sletting av opplysninger, fra alle medier opplysningene er lagret på, inklusive sikkerhetskopier.

Behandling av helseopplysninger er forankret i personopplysningsforordningen artikkel 9. Begrepet helse- og personopplysninger omfatter både direkte og indirekte identifiserbare opplysninger. Det inkluderer også kodede / aidentifiserte opplysninger. Se eget definisjonsdokument [Kilder og definisjoner i regionalt styringssystem for informasjonssikkerhet](#).

Databehandling		Etterlevd		
		JA	NEI	I/R
3.1.1.1	Det skal være besluttet og godkjent et formål med databehandlingen			
3.1.1.2	Det skal være opprettet og godkjent en tjenesteavtale og tjenestespesifikk databehandleravtale mellom Sykehuspartner og databehandlingsansvarlig			
3.1.1.3	Det skal være etablert en oversikt over alle informasjons-elementer som inngår i tjenesten			
3.1.1.4	Alle avvik fra regionale sikkerhetskrav skal godkjennes av alle foretakene i regionen som blir berørt av avviket			
3.1.1.5	Det skal dokumenteres hvorvidt en personvernkonsekvensvurdering er nødvendig, og hvor dette er nødvendig, skal personvernkonsekvensvurdering utarbeides			

3.1.1.6	Det skal dokumenteres behandlingens art, mengde, omfang, lagringstid og tilgjengelighet knyttet til personopplysninger, samt sletterutiner for disse			
3.1.1.7	Det skal uttømmende fremkomme fra hvilke land databehandlingen utføres fra, herunder bruk av tredjeland, og bruken skal være vurdert opp mot personvernet			
3.1.1.8	Ved bruk av databehandling fra tredjeland, skal EUs standardpersonvernbestemmelser benyttes			
3.1.1.9	Det skal være definert en systemeier og tjenesteansvarlig for behandlingen			

3.1.2 Leverandørstyring

Med leverandørstyring menes tiltak knyttet til å sikre at leverandører etterlever prinsipper og krav nedfelt i dette dokumentet. Med leverandører menes ekstern tredjepart som utfører databehandling, vedlikehold, service, drift, forvaltning eller lignende på vegne av virksomheten.

Leverandørstyring		Etterlevd		
		JA	NEI	I/R
3.1.2.1	Alt innleid personell, samt ansatte hos leverandører som utfører tidsbegrenset arbeid på vegne av virksomheten skal signere sikkerhetsinstruks			
3.1.2.2	Alle leverandører og underleverandører 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			
3.1.2.3	Alle leverandører og underleverandører som skal behandle helse- og personopplysninger skal kunne dokumentere egen informasjonssikkerhet iht. ISO 27001			
3.1.2.4	Alle leverandører og underleverandører som skal behandle helse- og personopplysninger skal ha opprettet personvernombud jfr GDPR artikkel 37 og personopplysningsloven § 19			
3.1.2.5	All leverandørtilgang skal gjøres gjennom Virksomhetens leverandørportal			

3.1.2.6	For at en leverandør og underleverandør skal kunne gis utvidede behovsbaserte rettigheter må det foreligge en godkjent risikovurdering			
3.1.2.7	Leverandører kan ikke flytte eller kopiere data ut eller inn fra IKT-utstyr i Virksomhetens nettverk, uten at det foreligger en godkjent risikovurdering			
3.1.2.8	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.			
3.1.2.9	Ved opphør av kontrakt plikter leverandør å følge instruks for terminering som beskrevet i databehandleravtale			

3.1.3 Anskaffelser

Med anskaffelser menes prosessen knyttet til innkjøp av tjenester i forbindelse med databehandling. Ved anskaffelser skal virksomheten(e) ivareta at leverandører og utstyr i best mulig grad etterlever sikkerhetsprinsippene beskrevet i dette dokumentet.

Anskaffelser		Etterlevd		
		JA	NEI	I/R
3.1.3.1	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)			
3.1.3.2	Anskaffelser fra tredjeland som innebærer behandling av personopplysninger må særskilt prøves, før databehandlingen kan godkjennes			
3.1.3.3	Anskaffelsen er i tråd med HSØ sine sikkerhetsprinsipper, inkludert dette dokumentet og øvrige dokumenter i HSØs styringssystem for informasjonssikkerhet.			
3.1.3.4	Utforming, drift, bruk og administrasjon av informasjonssystemer samstemmer med aktuelle lov(er), forskrift(er) og kontraktsfestede krav til sikring.			
3.1.3.5	Anskaffelsen/systemet med underliggende komponenter skal supporteres i kontraktsperiodens levetid			

3.1.3.6	Anskaffelser av tjenester og utstyr underlagt sikkerhetsloven og forskrifter, må særskilt behandles.			
---------	--	--	--	--

3.2 Tilgangsstyring

Andre avsnitt omhandler prinsipper for å sikre at det gis tilgang til data og helse- og personopplysninger i henhold til dokumentert tjenstlig behov.

Dette avsnittet består av fem underavsnitt: Identifisering, autentisering, autorisering, sporbarhet og sperring.

3.2.1 Identifisering

Med identifisering menes tiltak for å håndtere hvem og hva en person er. En digital identitet kan ha en eller flere brukerkontoer.

Identifisering		Etterlevd		
		JA	NEI	I/R
3.2.1.1	Det skal kun benyttes personlige brukere. Fellesbrukere eller på annen måte deling av brukerkontoer skal ikke forekomme.			
3.2.1.2	Alle kontoer skal entydig knyttes opp mot en digital identitet, og ivareta kravene om uavviselighet og sporbarhet ved autentisering.			

3.2.2 Autentisering

Med autentisering menes 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. I henhold til pasientjournalloven § 22 skal det være tilgangsstyring, logging og etterfølgende kontroll.

Autentisering		Etterlevd		
		JA	NEI	I/R
3.2.2.1	Autentisering skal gjøres mot sentral autentiseringsløsning (IAM) ihht. sikkerhetsprinsipper og krav for IAM .			
3.2.2.2	Autentisering skal støtte identitetsutveksling ved hjelp av SAML forsterket med kryptografisk signering, eller tilsvarende.			
3.2.2.3	Passord skal transporteres kryptert etter gjeldende policy i Helse Sør-Øst .			

3.2.2.4	Passord skal lagres som hash etter gjeldende policy i Helse Sør-Øst .			
3.2.2.5	Systemet skal kunne håndheve vedtatt instruks for passordkompleksitet .			
3.2.2.6	Passord skal aldri oppbevares skriftlig, annet enn i godkjent hvelv.			
3.2.2.7	Regelmessige og planlagte oppgaver på IKT-systemene skal kjøres av servicekontoer. Servicekontoer skal standardiseres og herdes ihht herding av systemer og tjenester.			
3.2.2.8	Autentiseringen må ha tilstrekkelig styrke ihht gjeldende policy i Helse Sør-Øst.			
3.2.2.9	Det skal benyttes to-faktorautentisering ved: <ul style="list-style-type: none"> · Tilgang fra eksterne nettverk (ekstranett, Internett, leverandører). · Tilgang fra klientnettverk mot drift, forvaltning og adminløsninger. 			
3.2.2.10	Passordhvelv skal benyttes for alle ikke-personlige kontoer så som service- og administratorkontoer.			
3.2.2.11	Informasjonssystemer skal støtte Single Sign-On (SSO).			
3.2.2.12	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).			
3.2.2.13	Applikasjonen skal ha egen tilgangskontroll, med autentisering og autorisering mot sentral tjeneste.			
3.2.2.14	Avsender skal kunne digitalt signere utvalgte dokumenter med kvalifisert sertifikat.			

3.2.3 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 tilgangsstyring for behandlingsrettede helseregistre. Dette gjelder for både virksomhetsinterne og regionale journalsystemer. I pasientjournalloven § 22 står det at "Den dataansvarlige og databehandleren skal gjennomføre tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen, jf. personvernforordningen artikkel 32. Den dataansvarlige og databehandleren skal blant annet sørge for tilgangsstyring, logging og etterfølgende

kontroll.”. Pasientjournalloven § 19 gjelder tilgjengeliggjøring av helseopplysninger dvs. informasjonsdeling mellom helsepersonell i forbindelse med helsehjelp. I § 19 første ledd står det at “Innenfor rammen av taushetsplikten skal den dataansvarlige sørge for at relevante og nødvendige helseopplysninger er tilgjengelige for helsepersonell og annet samarbeidende personell når dette er nødvendig for å yte, administrere eller kvalitetssikre helsehjelp til den enkelte.”

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.

Autorisering		Etterlevd?		
		JA	NEI	I/R
3.2.3.1	Brukerkontoer skal ikke gis administrative rettigheter. For behovsbaserte formål skal separate personlige kontoer med utvidede rettigheter opprettes.			
3.2.3.2	Tilganger skal være basert på rollestyring.			
3.2.3.3	Tilganger skal være på et lavest mulig nivå iht. dokumentert behov.			
3.2.3.4	Tilganger til personopplysninger skal begrenses til behov knyttet til brukerens roller og organisasjonstilhørighet.			
3.2.3.5	Privilegerte tilganger tildeles kun når det foreligger gyldig grunnlag for databehandling.			
3.2.3.6	Privilegerte tilganger tildeles kun i henhold til tjenestlig og dokumentert behov.			

3.2.4 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 informasjons-element er uendret, og at det entydig kan knyttes til en bestemt digital identitet. Uavviselighet er i mange sammenhenger også omtalt som ikke-benektning. Uavviselighet benyttes også i sammenheng med autorisering og autentisering.

I henhold til pasientjournalloven § 22 skal det være tilgangsstyring, logging og etterfølgende kontroll. Bruk av informasjonssystem skal dokumenteres. Dette følger av pasientjournalloven § 22. Det stilles videre krav om at loggene skal kontrolleres.

Det følger av pasientjournalloven § 18 at “Pasienten eller brukeren har rett til informasjon og innsyn i henhold til pasient- og brukerrettighetsloven § 3-6 tredje ledd og § 5-1 og til personvernforordningen artikkel 13 og 15”

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

Sporbarhet		Etterlevd		
		JA	NEI	I/R
3.2.4.1	<p>Alle relevante handlinger skal logges. Relevante handlinger skal måles opp mot informasjonssystemet, men som et minimum skal følgende logges:</p> <ul style="list-style-type: none"> • 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. 			
3.2.4.2	<p>Alle IKT-systemer skal logge hendelser i et standardisert format, i tråd med beste praksis for det enkelte IKT-systemet.</p> <p>Formålet er å sikre at logger beholder samme format og lesbarhet uavhengig av programvareversjoner og -oppdateringer, at loggene er ikke krever spesialprogramvare for å leses, og at loggene er formatert på en måte som legger til rette for autoamtisk korrelering og logganalyse.</p>			
3.2.4.3	Alle IKT-systemene skal tilgjengeliggjøre logger for gjennomgang og eksport.			
3.2.4.4	Logger som er relevante for informasjonssikkerheten skal kunne overføres til sentralt loggmottak.			
3.2.4.5	Logger skal tilgangsstyres slik at de beskyttes mot manipulering/endring.			
3.2.4.6	Logger skal ha tidsstempling og klokken benyttet til tidsstemplingen skal være synkronisert mot sentral NTP-tjeneste.			
3.2.4.7	Før databehandling iverksettes skal det være avklart at logger gjennomgås manuelt eller automatisk basert på forhånds-definerte kriterier med det formål å avdekke mulige sikkerhetsavvik.			

3.2.4.8	Logger skal oppbevares i tråd med krav. Som minimum gjelder 24 måneders lagring for sikkerhetslogger, lagring utover dette må spesifiseres i avtale. For pasientjournallogger eller andre logger knyttet til behandlingsrettede registre, gjelder egne krav.			
3.2.4.9	Tilganger skal loggføres. I tillegg skal endringer i tilganger og hvem som beslutter endringer i disse også loggføres.			
3.2.4.10	Bruk av privilegerte tilganger i systemer i HSØ er uavviselig.			

3.2.5 Sperring

Med sperring menes den enkelte pasients rett til å 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, samt for at sperrede opplysninger skal kunne åpnes enten etter pasientens eget ønske eller dersom behandler vurderer at det foreligger "tungtveiende grunner" etter pasient- og brukerrettighetsloven § 5-3.

I Pasientjournalloven § 7 litera c står det 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»

I Pasientjournalloven § 17 står det at «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:

- Journalansvarlig 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. Journalansvarlig er 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.
- 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 hvilken informasjon det skal begrenses innsyn i.

Tabellen under gir 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.

Sperring		Etterlevd		
		JA	NEI	I/R
3.2.5.1	Det skal være mulig i et behandlingsrettet helseregister og etter forespørsel fra en pasient, å kunne begrense tilgangen til vedkommendes pasientjournal til definerte enkeltpersoner, enkeltroller og/eller enkeltgrupper.			
3.2.5.2	Begrensning i tilgang til journal herunder dokumenter og dokumenttyper skal kunne avgrenses i tid.			
3.2.5.3	Det skal være mulig i et behandlingsrettet helseregister og etter forespørsel fra en pasient, å kunne sperre eller begrense tilgangen for alle opplysninger knyttet til en pasientbehandling.			

3.3 Teknisk sikkerhet

Tredje avsnitt omhandler prinsipper for å etablere tekniske tiltak for å beskytte data og helse- og personopplysninger.

Dette avsnittet består av seks underavsnitt: Infrastruktursikkerhet, klientsikkerhet, serversikkerhet, applikasjonssikkerhet, angrepsflate og terminering.

3.3.1 Infrastruktursikkerhet

Med infrastruktursikkerhet menes de tiltakene som er implementert for å oppnå akseptabel risiko for infrastrukturen.

Infrastruktursikkerhet		Etterlevd		
		JA	NEI	I/R
3.3.1.1	Tjenesten kan etableres på Sykehuspartners infrastruktur			
3.3.1.2	Tjenesten kan etableres ihht Sykehuspartners sonemodell			

3.3.2 Klientsikkerhet

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

Klientsikkerhet		Etterlevd		
		JA	NEI	I/R
3.3.2.1	Klienter skal leveres av Sykehuspartner. Hvis ikke dette er mulig, gjelder etterfølgende likevel krav fra og med 3.3.2.2 til og med 3.3.2.9.			
3.3.2.2	Klienter som ikke er levert gjennom Sykehuspartner skal sonemessig segmenteres fra klienter levert av Sykehuspartner.			
3.3.2.3	Klienter skal ha kryptert harddisk.			
3.3.2.4	Klienter skal ha automatisk installasjon av sikkerhetsoppdateringer og antivirussignaturer.			
3.3.2.5	Klienter skal ha automatisk låsing av skjerm m/ passord.			
3.3.2.6	Brukere skal ikke ha administrasjonsprivilegier på egen klient. Brukere skal ikke kunne deaktivere lokale sikkerhetskontroller.			
3.3.2.7	Klienter skal kun ha godkjent og risikovurdert programvare installert.			
3.3.2.8	Klienter skal alltid benytte VPN når man er utenfor Virksomhetens infrastruktur, for eksempel private eller offentlige nettverk.			
3.3.2.9	Klienter skal autentiseres gjennom klientsertifikater for å kunne koble seg på Virksomhetens nettverk.			

3.3.3 Serversikkerhet

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

Serversikkerhet		Etterlevd		
		JA	NEI	I/R
3.3.3.1	Server skal leveres av Sykehuspartner. Hvis ikke dette er mulig, gjelder etterfølgende krav fra 3.3.3.2 til og med 3.3.3.7.			
3.3.3.2	Server skal sonemessig segmenteres fra server levert av Sykehuspartner.			
3.3.3.3	Serveren skal som minimum herdes i tråd med instruks fra Sykehuspartner. Ved konflikt i kravsett mellom			

	applikasjonsleverandør og Sykehuspartner, skal det gjennomføres risikovurdering.			
3.3.3.4	Serveren skal ha installert gjeldende sikkerhetsoppdateringer og antivirussignaturer innen rimelig tid iht. kritikalitet.			
3.3.3.5	Serveren skal inngå i driftsovervåkingen.			
3.3.3.6	Serveren skal synkronisere klokken mot sentral NTP-server.			
3.3.3.7	Bruk av ressurser skal inn i regime for overvåking og justering, og det skal foretas beregninger over framtidige kapasitetsbehov for å sikre at systemet oppnår påkrevd ytelse.			

3.3.4 Applikasjonssikkerhet

Med applikasjonssikkerhet menes de tiltakene som er implementert i de tjenestene som benyttes for å utføre databehandlingen.

Applikasjonssikkerhet		Etterlevd		
		JA	NEI	I/R
3.3.4.1	Applikasjonen skal ha definert applikasjonsforvaltning i tråd med regionale føringer, hvor roller og ansvar mht. forvaltning av applikasjonen er avklart.			
3.3.4.2	Det skal legges til rette for effektiv og hurtig installasjon av sikkerhetsoppdateringer.			
3.3.4.3	Applikasjonen skal benytte en trelagsarkitektur for å begrense eksponering av bakenforliggende database.			
3.3.4.4	Applikasjonen skal følge etablert endrings- og oppdaterings-regime for operativsystemet.			
3.3.4.5	Applikasjonen skal støtte utskrift via Sikker Print.			
3.3.4.6	Applikasjonen skal aldri lagre eller overføre passord i klartekst, jf. 3.2.2.4			
3.3.4.7	Applikasjonen skal kryptere data som går i transitt i henhold til kryptoinstruksen .			
3.3.4.8	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.			

3.3.5 Sikkerhetskonnfigurasjon av MS SQL-databaser

MS SQL-databaser som innføres i Sykehuspartner HF skal være konfigurert i tråd med følgende anbefalinger. Om en applikasjon/database ikke støtter mekanismene under, skal det fylles ut «NEI» i tabellen under, og årsaken for at mekanismen ikke støttes skal redegjøres for.

Det er Sykehuspartner HF v/ Databasedrift som er ansvarlig for kravspesifikasjon for oppsett av MS SQL.

Sikkerhetskonnfigurasjon MS SQL		Etterlevd		
		JA	NEI	I/R
3.3.5.1	Ensure 'Ad Hoc Distributed Queries' Server Configuration Option is set to '0'			
3.3.5.2	Ensure 'CLR Enabled' Server Configuration Option is set to '0'			
3.3.5.3	Ensure 'Cross DB Ownership Chaining' Server Configuration Option is set to '0'			
3.3.5.4	Ensure 'Ole Automation Procedures' Server Configuration Option is set to '0'			
3.3.5.5	Ensure the 'sa' Login Account is set to 'Disabled'			
3.3.5.6	Ensure 'xp_cmdshell' Server Configuration Option is set to '0'			
3.3.5.7	Ensure 'Server Authentication' Property is set to 'Windows Authentication Mode'			
3.3.5.8	Ensure 'Orphaned Users' are Dropped From SQL Server Databases			
3.3.5.9	Database default file location for all user databases, according to Sykehuspartner's standard: Data: E:\MSSQLUserDB\ Log: F:\MSSQLUserLog\			
3.3.5.10	State that the application user, do not need higher right's than DB_OWNER			
3.3.5.11	Regarding upgrade of the Application/database, state that there are no need for use of SA or members of SYSADMIN role			

3.3.6 Angrepsflate

Med angrepsflate menes de tiltakene som er implementert på de tjenestene og serverne som virksomheten eksponerer mot Internett og som dermed utgjør virksomhetens digitale fotavtrykk.

Angrepsflate		Etterlevd		
		JA	NEI	I/R
3.3.6.1	Alle tjenester som eksponeres eksternt skal penetrasjonstestes, uavhengig av sikkerhetsnivå.			
3.3.6.2	Alle tjenester som eksponeres eksternt skal plasseres i virksomhetens DMZ.			
3.3.6.3	Kommunikasjon skal alltid initieres av tjenesten i det høyeste sikkerhetsnivået.			

3.3.7 Terminering

Med terminering menes tiltakene som er implementert i tilknytting til utfasing av applikasjon og utskiftning av IKT-utstyr. Terminering innebærer at applikasjonene/utstyret ikke lenger vil inngå i informasjonsbehandlingen i virksomheten, og at applikasjonene/utstyret enten skal destrueres, resirkuleres, selges, leveres tilbake til leasing leverandør, gis bort eller på annen måte terminere det juridiske eierskapet hos virksomheten.

4.6 Terminering		Etterlevd		
		JA	NEI	I/R
3.3.7.1	Avhending av utstyr skal skje i henhold til instruks			
3.3.7.2	Ved terminering av tjenesten skal: -brannmursåpninger lukkes -brukerkontoer deaktiveres -system og administratorkontoer fjernes -leverandørtilgang fjernes -Tjenesten settes inaktiv i tjenestekatalogen			

3.4 Forvaltning

Fjerde avsnitt omhandler prinsipper for å sikre at IKT-tjenester og utstyr blir forvaltet slik at det skal fungere i tråd med hensikt og formål i den avtalte levetid.

Dette avsnittet består av to underavsnitt: Drift og dokumentasjon.

3.4.1 Drift

Med drift menes de tiltakene som er implementert for å sikre at personell kan sørge for at tjenestene som leveres er sikre og stabile.

Drift		Etterlevd		
		JA	NEI	I/R
3.4.1.1	Administrasjon av virksomhetens servere og tjenester skal gjøres gjennom en egen administrasjonsinfrastruktur med tofaktorausautentisering.			
3.4.1.2	Administrasjonsinfrastruktur skal ikke ha tilgang til Internett eller andre eksterne nettverk.			
3.4.1.3	Enhver AD gruppe skal ha en eier som har forvaltningsansvaret.			
3.4.1.4	Forvaltning av privilegerte tilganger er en del av helhetlig sikkerhetsarkitektur.			
3.4.1.5	All bruk av privilegerte tilganger skjer igjennom en helhetlig driftsløsning for HSØ.			
3.4.1.6	Bruk av privilegerte tilganger er mulig i HSØ til enhver tid uavhengig av hendelser i det ordinære produksjonsmiljøet.			

3.4.2 Dokumentasjon

Med dokumentasjon menes de tiltakene som er implementert for å sikre at virksomheten skal dokumentere informasjonssystemene sine, inkl. konfigurasjon.

Dokumentasjon		Etterlevd		
		JA	NEI	I/R
3.4.2.1	Det skal være etablert rutiner for tjenesten, der rutinene for henholdsvis bruk og forvaltning er innbyrdes harmonisert.			
3.4.2.2	Endringer i en tjeneste skal dokumenteres i systemdokumentasjonen.			
3.4.2.3	Systemdokumentasjon skal være lagret og holdes oppdatert på godkjent område for oppbevaring i minst fem år etter siste endring.			
3.4.2.4	Det skal være opprettet planer for business continuity og disaster recovery for systemer som er definert som kriticalitet 1.			
3.4.2.5	Det skal gjennomføres opplæring i policy og prosedyrer som er relevant for alle roller i systemet. Dette innbefatter samtlige brukere og administratorer av systemet, samt eventuelle kontraktører og tredjepartsbrukere.			

3.5 Annet

Fyll inn annen relevant informasjon om systemet/tjenesten:

4 Definisjoner

Se eget dokument: [Kilder og definisjoner i regionalt styringssystem for informasjonssikkerhet](#)

5 Avvik eller dissens

Avvik på denne instruks meldes i virksomhetens avvikssystem. Informasjonssikkerhetsleder og/eller personvernombud skal varsles.

6 Referanser

- Se eget dokument: [Sikkerhetsregulerende lovverk gjeldende for helseforetaksgruppen](#)
- Prinsippene for anvendelse og forvaltning av dokumentet er beskrevet i dokumentet [Overordnede prinsipper for regionalt styringssystem for informasjonssikkerhet](#).
- Sikkerhetsprinsipper og krav for IAM