HELSE SØR-ØST

Sikkerhetsprinsipper og -krav for IKT-infrastruktur og applikasjoner

Versjonsnummer	**Dato**	**Godkjent av**
1.0	22.12.2016	Cathrine Marie Lofthus
1.1	23.10.2018	Cathrine Marie Lofthus

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 foretaksvise 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 lovhjemmel 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, sikkerhetsledere, regionalt sikkerhetsforum, 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. Ved anskaffelse av applikasjoner og tjenester, og spesielt behandlingsrettede helseregistre, er deler av kravene spesifikt rettet mot behandlingsrettede helseregistre, deler av kravene vil være direkte nødvendige for å avklare grensesnitt mot eksisterende tjenester og infrastruktur, og deler av kravene er mer perifere.

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 og godkjennes av Regionalt sikkerhetsfaglig råd (RSR) eller respektive informasjonssikkerhetsleder som er berørt dersom unntak kun berører et eller noen helseforetak.

- 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 med forskrift.
- **Ledere** på alle nivåer har ansvar for oppfylling av instruksen 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 Fremgangsmåte

3.1 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 helse- og personopplysninger 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			

3.2 Behandling av helse- og personopplysninger

Med behandling av helse- og personopplysninger menes all registrering, prosessering, bruk og lagring som gjennomføres. 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 helse- og personopplysninger er forankret i personopplysningsloven § 15.
- Begrepet helse- og personopplysninger omfatter både direkte og indirekte identifiserbare opplysninger. Det inkluderer også kodede / avidentifiserte opplysninger. Se eget definisjonsdokument Kilder og definisjoner i regionalt styringssystem for informasjonssikkerhet.

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 og databehandlingsansvarlig			
2.3	Det skal være opprettet og godkjent databehandleravtaler med eventuelle underleverandører			

3.3 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 Pasientjournalloven § 22		Etterlevd?		
		JA	NEI	I/R
3.10	Arbeidsforholdet[1][2] 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[3] 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[4])			

[1] Dette kan løses på ulike måter f.eks. vha en kombinert primærnøkkel som alltid består av en ansatt- og en organisasjonsidentifikator.

[2] Arbeidsforholdet omfatter både fast- og deltidsansatte, samt innleide og andre som foretaket har ordnet formell instruksjonsrett over for og registrert i HR-systemet (Personalportalen).

[3] 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

[4] For tiden er RESH den autoritative datakilden for organisasjonsenheter i spesialisthelsetjenesten https://helsedirektoratet.no/helseadministrative-registre/register-for-enheter-i-spesialisthelsetjenesten-resh

3.4 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			

3.5 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.			

3.6 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. I henhold til pasientjournalloven § 22 skal det 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 [1].			
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[2].			
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[3]			
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)			

[1] https://www.regjeringen.no/nb/dokument/dep/kmd/lover_regler/retningslinjer/2008/rammeverk-for-autentisering-og-uavviseli/4/id505929/

[2] https://www.regjeringen.no/nb/dokument/dep/kmd/lover_regler/retningslinjer/2008/rammeverk-for-autentisering-og-uavviseli/4/id505929/

[3] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

3.7 Autorisering (tilgangsstyring)

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 databehandlingsansvarlige og databehandleren 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 § 19 gjelder tilgjengeliggjøring av helseopplysninger dvs. informasjonsdeling mellom helsepersonell i forbindelse med helsehjelp. I § 19 første ledd står det at "Innenfor rammen av taushetsplikt skal den databehandlingsansvarlige sørge for at relevante og nødvendige helseopplysninger er tilgjengelige for helsepersonell og annet samarbeidende helsepersonell når dette er nødvendig for å yte, administrere og kvalitetssikre helsehjelpen 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.

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			

	Etterlevd?

Spesielt for behandlingsrettede helseregistre PJL §22 POL§13 POF §§ 2-1, 2-11, 2-12, 2-13, 2-14		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 [1]brukeren har i sitt påloggede arbeidsforhold.			
7.7	Rollen [2] 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 [3]den ansatte innehar i et behandlingsrettet helseregister skal skille dennes tilganger begrenset i forhold til pasienter i aktiv behandling [4]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[5] 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): hvilke sett av organisasjonsenheter pasienten tidligere har vært behandlet ved innen et foretak, eller hele foretaket under ett			

	hvilke sett av organisasjonsenheter pasienten tidligere har vært behandlet ved på tvers av flere foretak, eller inkludert et eller flere hele foretaket gitte diagnoser/kombinasjoner av diagnoser, eller alle diagnoser antall måneder/år tilbake i tid for når pasienten ble behandlet av gitt org.enhet inkluder døde pasienter ja/nei 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: pasienter som har vært behandlet ved gitte sett av organisasjonsenheter innen et foretak, eller hele foretaket under ett pasienten som har vært behandlet ved gitte sett av organisasjonsenheter på tvers av flere foretak, eller et eller flere foretaket pasienter med valgt kombinasjon(er) av diagnose- og prosedyrekoder, eller alle diagnoser antall måneder/år tilbake i tid for når pasienten ble behandlet av gitt org.enhet inkluder døde pasienter ja/nei pasienter i et gitt pasientforløp			
7.15	Det skal være mulig å entydige identifisere hvem som er juridisk[6]- og/eller medisinsk ansvarlig [7]for en gitt pasienten innen en juridisk enhet og på tvers av juridiske enheter involvert i pasientens behandling.			

[1] Rollen brukeren har er definert i den regionale rollemodellen f.eks. «lege», «sykepleier», «farmasøyt», osv.

[2] Det forutsettes at den enkelte ansatt/innleide kan ha ulike roller i ulike arbeidsforhold

[3] Tidsperspektivet må enkelt kunne endres og varieres avhengig av rolle.

[4] Inneliggende og poliklinikk.

[5] Pasienter som ikke har noen aktive forhold til foretak

[6] Med juridisk ansvar menes den organisasjonsenheten som juridisk har ansvaret for pasientens behandling

[7] Med medisinsk ansvar menes den legen eller psykolog som er pasientansvarlig

3.8 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			

3.9 Sperring

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. 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 hva det /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.

Spesielt for behandlingsrettede helseregistre PJL §§7c og 17, første ledd bokstav a og ande ledd		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.			

3.10 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			

3.11 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.

I henhold til pasientjournalloven § 22 skal det 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.

Det følger av pasientjournalloven § 18 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: pålogging utlogging åpning av pasientjournal lesing i pasientjournal skriving i pasientjournal sletting» av opplysninger i pasientjournal sperring av pasientjournal fletting utskrift oppretting og endring av tilganger og rettigheter kopiering og sletting av brukerroller eksport av datasett søk som er gjort			
11.10	Følgende informasjon skal minimum lagres ved tilgang og aktivitet i et behandlingsrettet helseregister: Bruker, og hvilken av brukerens roller som var aktiv, som har forsøkt utført eller gjennomført tilgang/enhver form for aktivitet Dataelement endret			

	Om dataelement endret er opprettet, lest, endret, skrevet ut, slettet eller annen aktivitet som det er mulig for autoriserte å gjennomføre Tidspunkt for gjennomføring/hendelsen 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			

3.12 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 georedundans			

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			

3.13 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 uten at det foreligger en godkjent risikovurdering (gjelder ikke gjestenettverk).			
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.			

3.14 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			

3.15 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.			

3.16 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			

3.17 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.			

3.18 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			

18.6	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. Se eget dokument: Fellesregional kryptopolicy.			

3.19 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			

3.20 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			

3.21 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.			

3.22 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			

3.23 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 fulgt?			
23.3	Følger tjenesten lovkravene til universell utforming 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.			

3.24 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			

3.25 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 .