SJUKEHUSAPOTEKA **VEST HF**

STYRESAK

GÅR TIL:	Styremedlemmer
FØRETAK:	Sjukehusapoteka Vest
DATO:	24.05.2018
SAKSHANDSAMAR:	IKT leiar Jimmy Thomsen og Økonomidirektør Ola Rye
SAKA GJELD:	**Leiinga sin årlege gjennomgang av informasjonstryggleik**
ARKIVSAK:	
STYRESAK:	**021/18**
STYREMØTE:	**31.05.2018**

FORSLAG TIL VEDTAK
Styret tek saka til etterretning.

Oppsummering

SAV har implementert regionalt styringssystem for informasjonssikkerheit som ein integrert del av styring og forvaltning av IKT området. Styringssystemet har vore handsama av SAV leiarmøte og leiarmøtet har gjennomført leiinga si årlege gjennomgang av informasjonssikkerhet, sist gong 6. mars 2018. SAV har nytta malverket i styringssystemet i arbeidet. Leiinga sin årlege gjennomgang av informasjonssikkerhet er teken inn i årshjul for IKT området i SAV.

Arbeid med informasjonssikkerhet i SAV heng tett saman med status og tiltak innan tilsvarande arbeid i Helse Vest og Helse Vest IKT. Grunnlaget for leiinga sin årlege gjennomgang vert difor utarbeida i samarbeid med Helse Vest IKT og regionalt sikkerhetsutvalg (SU).

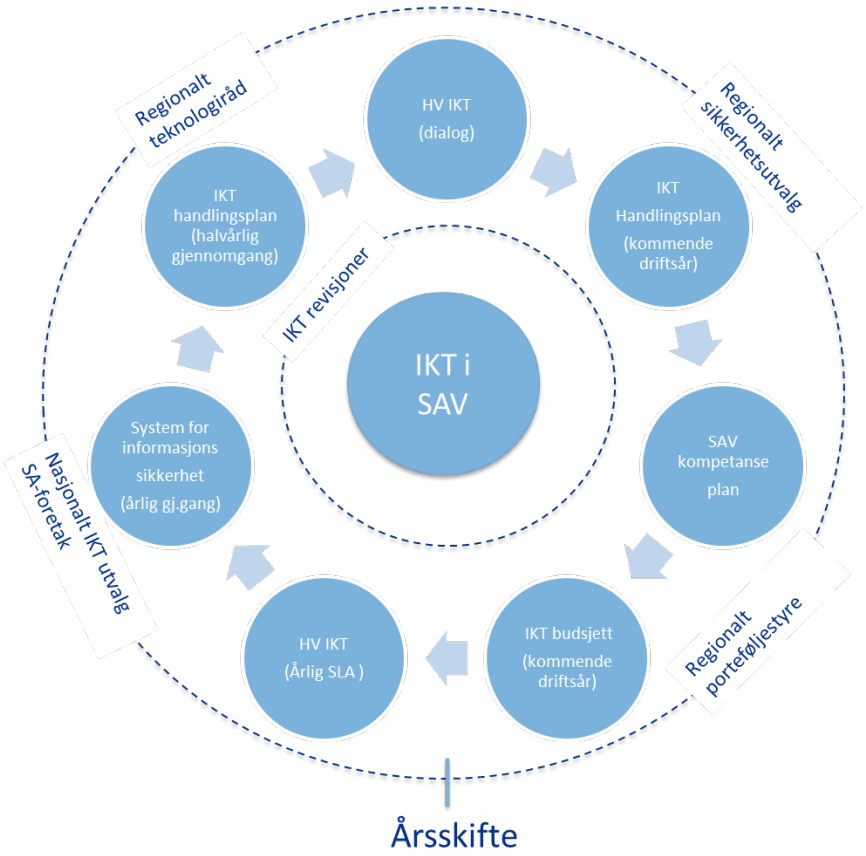
Leiinga sin gjennomgang av informasjonssikkerhet har avdekka forhold knytt til mellom anna behov for tettar oppfølging av leverandør for lagerrobotar med omsyn til overvaking (predictive service) og behov for etablering av nye databehandlaravtalar mellom anna ved konsernintern utsetting av systemansvar.

Auka merksemd på styringssystemet og bruk av malen ved leiinga si gjennomgang har betra kvaliteten på arbeidet med informasjonssikkerheit i SAV. Funn i leiinga sin gjennomgang er dokumenterte og føreslegne tiltak vert tekne inn i IKT handlingsplan og følg opp gjennom halvårleg handsaming av status i SAV si leiargruppe.

Fakta

Arbeidet med informasjonssikkerhet i SAV

Arbeidet med informasjonssikkerheit i SAV er ein integrert del av styring og forvaltning av IKT området i føretaket og kan skisserast i form av eit årshjul;



Figur 1 Årshjul for IKT i SAV

SAV sin systemportefølje blir påverka av nasjonale prosjekt og tiltak, samt regionale føringar mellom anna ved regional porteføljestyring, regionalt arkitektur kontor (RAK) og regionalt teknologiråd, tidlegare SIKT (Strategisk IKT). Regionalt teknologiråd er og arkitekturstyre og overordna arkitekturmål gjev føringar for at å få til ein systemportefølje som understøttar arbeidsprosessane på ein heilskapleg måte, og kor både arbeidsprosessar, informasjonshandtering og systemlandskap er beskrivne og dokumenterte. SAV har representasjon i teknologirådet ved økonomidirektør.

Nasjonalt IKT utval for sjukehusapotekføretak er eit fora der IKT leiarane i sjukehusapotekføretaka møtes for å samordna nasjonale initiativ og fremja nasjonalt samarbeid på IKT området. I dei mange endringsprosessane som apotekbransjen nå går igjennom, har dette utvalet ein viktig funksjon.

SAV deltek i Regionalt sikkerheitsutval (SU) ved IKT sikkerheitsansvarleg/IKT leiar. SU har som mandat å vera rådgjevande organ for informasjonssikkerheit i Hese Vest og med eit særleg ansvar for forvaltning av styringssystem for informasjonssikkerheit.

Ved inngangen til nytt år vert årlege IKT handlingsplan for SAV presentert for HV IKT si leiargruppe i dialogmøte og med dette vert SAV sine mål og tiltak på IKT området forankra hjå HV IKT. I dette møtet er og årleg revisjon av SLA avtale mellom HV IKT og SAV på agenda. IKT Handlingsplan vert følgt opp i SAV si leiargruppe. Staus på tiltak vert og følgd opp med

eit nytt halvårleg møte med HV IKT. Mål og tiltak innan IKT området påverkar behov for kompetansebygging. SAV sin kompetanseplan blir gjennomgått og revidert for å implementere tiltak.

I byrjinga av nytt år blir leiinga sin gjennomgang av informasjonssikkerheit gjennomført. Dette gjev innspel til ny årleg IKT handlingsplan som igjen gjev innspel til budsjettarbeidet. IKT området inngår i SAV sin plan for interne revisjonar. Resultat frå revisjonar gjev innspel til tiltak IKT handlingsplan med mål om å lukke avdekka forhold.

Styringssystem for informasjonssikkerhet i SAV
SAV har implementert regionalt styringssystem for informasjonssikkerhet. Styringssystemet gjev både overordna og strategiske mål for sikkerheitsarbeidet, men og konkret rettleiing i form av IKT sikkerheitsinstruks og ein rekke prosedyrar og malar.

Årleg samsvarsvurdering skjer gjennom leiinga sin gjennomgang av informasjonssikkerheit slik dette er skissert i styringssystemet sitt malverk (*M04 Ledelsens gjennomgang av informassjonsikkerhet*). Her vert gjort ei vurdering om avvik og tiltak frå ROS analyser er handtert på ein tilfredsstillande måte, og om det overordna nivået av risiko er på eit akseptabelt nivå. Nokre tema i M04 peikar også på naudsynt oversikt og dokumentasjon i forhold til handsaming og lagring av personinformasjon, ut frå krav i gjeldande lovgjevnad og rettleiing i Normen for informasjonssikkerheit i helse- og omsorgssektoren.

Siste revisjon av styringssystem for informasjonssikkerheit vart handsama av SAV si leiargruppe 30.01.2018. Samsvarsvurdering vart gjennomført av leiargruppa 06.03.2018.

På eit dagleg operasjonelt nivå skjer sikkerheitsarbeidet gjennom avvikshandtering, ROS analyser og IKT revisjonar. Det daglege arbeidet dannar noko av grunnlaget for samsvarsvurderinga. Manglande samsvar blir i sin ende fanga opp som tiltak i IKT handlingsplan.

Føretaka i Helse Vest, irekna SAV, samarbeider tett om sikkerheitsarbeidet og Helse Vest IKT har ei viktig rolle i dette med årlege ROS analyser og revisjonar, kor kvart føretak blir involverte ved behov. Ved innføring av nye system, eller ved større endringar, er det obligatorisk med ROS analyse i samsvar med retningslinjer i styringssystemet.

IKT sikkerheitsarbeid dreier seg mykje om kompetanse og kultur som utgangspunkt for korleis vi handlar i kvardagen. Difor har SAV eit fokus på kompetansebygging som verkemiddel. Ut frå årleg IKT handlingsplan blir SAV kompetanseplan revidert innanfor IKT området.

Ansvar og roller i informasjonsikkerhetssarbeidet
Ansvar og roller er definerte i det regionale styringssystemet *(S04 – Sikkerhetsorganisering oversikt over funksjoner)*. SAV har teke dette i bruk og har konkretisert korleis rollene er implementerte i SAV. Eksempel på dette er at linjeleiarar med personalansvar skal sørge for at eige personell har riktige tilganger/ autorisasjonar/roller, at behandling av helse- og personopplysninger i eigen avdeling er meldt til rette instanser, at det er gjennomført obligatorisk sikkerhetsopplæring og at sikkerhetskrav blir overheldne og at avvik blir handsama i samsvar med verksemda sine rutiner. Linjeleiar skal og ha gjort seg kjent med beredskapsplaner for bortfall av IKT.

Samsvarsvurdering – leiinga sin gjennomgang av informasjonssikkerheit
Styringssystem for IKT sikkerheit har som målsetnad at handtering av personinformasjon, og særleg helseopplysningar skal handterast i samsvar med lov og forskrift. God kontroll fordrar medviten, og god oversikt og dokumentasjon.

I leiinga sin gjennomgang av IKT sikkerheit, er ein i samhøve med M04 innom følgjande tema:
- Resultat frå avvikshandtering
- Resultat frå sikkerheitsrevisjonar
- Resultat frå risikovurderingar
- Styringssystem for IKT sikkerheit (behov for tilpassingar og avklaringar)
- Nivå av akseptabel risiko (raude og gule punkter i risikovurderingar som ikkje er tilstrekkelig handtert)
- Ansvarsforhold og organisering med omsyn til sikkerheit
- Formål med behandling av personopplysingar
- Konfigurasjonskart over informasjonssystem
- Kontroll og oppfølging av inngåtte avtaler
- System med personopplysningar
- Resultat frå tilsyn
- Behov for endringar / plan for sikkerheitsarbeidet kommande år

Gjennomgangen viste mellom anna desse funna:

Område	**Funn**	**Føreslått tiltak**	**Omfang**
Databehandlar-avtaler	Det manglar avtaler mellom SAV og andre føretak i Helse Vest der SAV har sett ut systemansvarleg-rolla til t.d. Helse Bergen.	Databehandlaravtaler vert inngått med konserninterne føretak som vil definere hensikt med tilgang til personinformasjon.	Støttesystem for støtteprosessar, særleg innan HR området.
Dokumentasjon over formål med handtering av personinformasjon	Det manglar ein del på full oversikt på informasjon som handterast i støtteprosessane, til dømes for HR-prosessar, samt avklaring på forankring hjå datatilsynet for apotekdrifta.	Oppdatere oversikt informasjonselement. Avklare om dialog med datatilsynet er påkrevd (samarbeid meda Apotekforeningen).	Støtteprosessar, særlig HR, men også nokre avklaringar om personopplysningar i i apotekdrifta ovanfor datatilsynet.

Resultat ifrå ROS analyser	Det er gul-raude område frå ROS analyser på lager-robotar knytt til at proaktiv overvaking frå leverandør (Predictive Service) ikkje er implementert.	Etablere predictive service i samarbeid med leverandør og Helse Vest IKT med omsyn til tilgang via VPN mv. (Dette arbeidet har høg prioritet både hjå SAV og Helse Vest IKT)	Alle avdelingar med lagerobotar.

Årleg revisjonar utførde av HV IKT syner at det er ikkje er avdekka forhold som treff SAV.

Kommentar
Styringssystemet for informasjonssikkerheit er eit nyttig verktøy for å sikre ein systematisk gjennomgang av informasjonssikkerheitsarbeidet med omsyn til status og tiltak. Leiinga sin årlege gjennomgang legg grunnlaget for å vurdere kor ein skal leggja inn innsatsen for å betre informasjonssikkerhet og sikre at risikobildet er på eit akseptabelt nivå.

Konklusjon
SAV har implementert styringssystem for informasjonssikkerheit og gjennomført leiinga si gjennomgang av informasjonssikkerhet med utgangspunkt i malen i styringssystemet. Forankring av styringssystemet i leiinga har løfta merksemda og kvaliteten på intern kontroll innan informasjonssikkerheitsområdet i føretaket.