VEDLEGG 5 - STYRKET METODE FOR RISIKO- OG SÅRBARHETSVURDERINGER

Bakgrunn og formål

Foretaksmøtet vedtok den 31. mai at det skal utarbeides en plan for at *metodikk for risiko- og sårbarhetsanalyser knyttet til informasjonssikkerhet må gjennomgås, forsterkes og implementeres. Planen må ivareta informasjonssikkerhet og personvern innenfor lovmessige krav, samt de nye EU-personvernkravene (GDPR) som blir gjeldende fra mai 2018.*

Formålet med dette notatet er å overordnet beskrive plan for gjennomføring.

Leveranse

Sykehuspartner foreslår å etablere et prosjekt for forbedret metode og leveranse av risiko- og sårbarhetsvurderinger i Helse Sør-Øst.

Rapporten fra PwC peker på noen forbedringspunkter, men det vil være et overordnet mål å også bruke denne muligheten til å tydelig styrke Sykehuspartner HFs leveranseevne knyttet til risiko- og sårbarhetsvurderinger, ved å benytte verktøy for å betydelig redusere leveransetiden og – kompleksiteten sammenlignet med i dag. Et viktig første steg i en slik endring er å definere et målbilde på hvorfor vi utarbeider risiko- og sårbarhetsvurderinger, og hvordan rapportene best skal inngå i den øvrige virksomhetsstyringen.

Et tiltak som vil innføres i løpet av kort tid, vil være å forsterke oppfølgingen av risikoreduserende tiltak slikt at disse gjennomføres innenfor tidsmessig forventning. Tilsvarende på kort sikt vil det være et vesentlig metodeforbedringspunkt fra dagens håndtering av risiko- og sårbarhetsvurderinger er å gjennomføre vurdering av restrisiko, samt at det på noe lengre sikt også ses nærmere på kriteriene for å beslutte hvilke risikoreduserende tiltak som skal gjennomføres, slikt at det forholdsmessigheten mellom effekten av foreslåtte tiltak og kosten av å beslutte tiltakene blir mer synlig.

Dette mener vi vil medføre en signifikant bedring av Sykehuspartner HFs leveranseevne og det vil også styrke egen og regional risikostyring.

Vi ønsker å ta utgangspunkt i eksisterende regional prosess for risiko- og sårbarhetsvurderinger, og arbeide for å forbedre denne i henhold til både anbefalingene i den foreløpige rapporten fra gjennomgangen av iMod-programmet, Helse Sør-Øst RHF styresak 058-2017, samt også beste praksis fra andre referanser.

Prosjektet vil også ta eierskap til å etablere kvantitative, regionale risikoakseptkriterier, særlig innenfor konfidensialitet, samt knytte tilgjengelighetskrav opp mot etablert SLA. Det er også nødvendig for dette prosjektet å forbedre eksisterende mangel ved at informasjonssikkerhetsmessig risiko på enkelttjenester ikke inngår i den samlede risikostyringen for virksomheten, både i Sykehuspartner HF og til de øvrige helseforetakene i regionen

Det nye felleseuropeiske personopplysningslovverket (GDPR) gjøres gjeldende i Norge fra mai 2018, og arbeidet med dette vil inngå i planen. Det må bl.a. etableres metode, malverk og prosesser for utarbeidelse av personvernkonsekvenser og andre endringer som påvirker helsesektoren. Sykehuspartners GDPR-kompetanse vil på denne måten bidra til å heve etterlevelse i hele regionen.

Organisering

Leveransen foreslås organisert som et prosjekt. Det er ønskelig at prosjektet rapporterer til et prosjektstyre som består av fagpersoner også utenfor sikkerhetsmiljøet. Det er foreslått at HF-representasjon fra kundesiden deltar, samtidig som også Sykehuspartner-ledelse er representert. Det vil også etableres en refereansegruppe som vil inkludere Regionalt Sikkerhetsfaglig Råd.

Prosjektleder vil være overordnet ansvarlig for leveransen. Dette vil inkludere leveranser innen formål og gjennomføring med risiko- og sårbarhetsvurderinger, oppfølging inn i eksisterende prosesser for risikostyring og avviksregistrering, samt også å rapportere til prosjektstyret.

En tidlig leveranse vil være å utføre en gap-analyse mellom det som blir definert som et ønsket målbilde, og hva dagens metode for risiko- og sårbarhetsvurderinger gir.

Avhengigheter

Styrking av metode vil medføre kostnader til prosjektledelse og bruk av interne ressurser. Det har ikke vært rom til å gjennomføre en foranalyse som gir et kostnadsestimat til denne rapporten, men det bør tas høyde for at en forbedring av risiko- og sårbarhetsmetoden i Helse Sør-Øst vil ta noe tid og behøve flere runder med forankring i regionen. Det bør som minimum antas at 1 årsverk (FTE) for innleid ressurs.

For å også gi de leveransemessige gevinstene mener vi at det må anskaffes verktøy for å redusere kompleksitet og omfang jfr. dagens situasjon. Dette må redegjøres for på et senere tidspunkt.

Det er nødvendig med regional forankring – dagens risiko- og sårbarhetsvurderingsmetode er utarbeidet over tid, og dypt forankret i de enkelte helseforetakene. For at Sykehuspartner skal drive dette fremover, bør også mandatet forankres regionalt.

Neste milepæler

1. oktober 2017: En prosjektplan sammen med gap-analyse mellom nåsituasjon og målbilde presenteres ledergruppen i Sykehuspartner HF. Prosjektplanen vil beskrive hvordan styrking av risiko- og sårbarhetsmetode skal gjennomføres, basert på de føringene som er gitt i dette dokumentet. Videre iverksettes forsterket oppfølging av risikoreduserende tiltak.

1. november 2017: Forankring i Regionalt Sikkerhetsfaglig Råd for prosjektplan og målbilde, inkl. endring som medfører vurdering av restrisiko som del av malverket.

1. januar 2018: Eksisterende risikoregister gjennomgått, utestående tiltak tildeles oppfølgingsansvarlig gjennom avvikssystemet (DFS). Muliggjør rapportering og fremdriftsmåling fordelt på organisasjonsenhetene.

1. juni 2018: Endelig beslutning og innføring av ny regional metode for risiko- og sårbarhetsvurderinger.

Fakturaadresse:
Postboks 3562, 3007 Drammen
Besøksadresse hovedkontor:
Vektergården, Grønland 34
3045 Drammen

Telefon: 32 23 53 00
Telefaks: 32 23 53 01

Web: www.sykehuspartner.no
E-post: post@sykehuspartner.no
Org.nr.: 914637651