www.pwc.no

Helse Sør-Øst RHF

Foreløpig redegjørelse knyttet til IKT-tjenesteutsetting (iMod)

Helse Sør-Øst RHF, styremøte.

24. mai 2017

Innhold

1 Hovedkonklusjoner ... 3
2 Introduksjon ... 4
2.1 Bakgrunn ... 4
2.1.1 Infrastrukturmodernisering i Helse Sør-Øst ... 4
2.1.2 Leverandørmarkedet og IKT-tjenesteutsetting ... 4
2.1.3 ESN-avtalens omfang og sentrale milepæler ... 5
2.2 PwCs oppdrag ... 5
2.3 Grunnlag for foreløpig redegjørelse ... 6
3 Status i gjennomføringen av programmet ... 8
4 Kontrollregime knyttet til oppfyllelse av krav til informasjonssikkerhet ... 9
4.1 Sykehuspartner har ikke tilstrekkelig kontroll på tilgangsstyring ... 9
4.2 Sykehuspartner har ikke tilstrekkelig sporbarhet på tilganger til helseopplysninger ... 9
4.3 Minst 34 personer tilknyttet ESN-avtalen har hatt mulighet til å få tilgang til helseopplysninger ... 10
4.4 Beslutning om tilganger knyttet til ESN-avtalen burde vært eskalert ... 11
4.5 ESN har så langt ikke kunnet dokumentere at det foreligger databehandleravtaler med underleverandører 11
5 Systemet for gjennomføring av risikovurderinger knyttet til informasjonssikkerhet ... 13
5.1 Sentrale informasjonssikkerhetsrisikoer knyttet til ESN-kontrakten er ikke blitt tilstrekkelig vurdert ... 13
5.2 Svakheter i metodikk for risikovurderinger og uklarheter i beskrivelsen av nivå for akseptabel risiko innenfor informasjonssikkerhet ... 13
6 Om Helse Sør-Øst RHF har fått tilstrekkelig informasjon om risiko og gjennomføringen av programmet vedr. informasjonssikkerhet ... 16
6.1 Presentasjonen til styret i Helse Sør-Øst i sak 069-2016 vedrørende IKT-infrastrukturmodernisering var upresis og varsler om dette er ikke kommunisert til administrerende direktør i HSØ RHF ... 16

1 Hovedkonklusjoner

PwC har i perioden 4.-23. mai 2017 gjort undersøkelser knyttet til påstander om at eksterne tilganger til Helse Sør-Østs IKT-infrastruktur kan ha gitt tilgang til sensitive personopplysninger, herunder helseopplysninger. Tilgangene er knyttet til avtale om IKT-tjenesteutsetting inngått mellom Sykehuspartner HF og Enterprise Services Norge AS og pågående program i Sykehuspartner, iMod.

PwCs undersøkelser og vurderinger er knyttet til perioden fra Sykehuspartner HF fikk oppdraget med å inngå kontrakt og gjennomføre programmet på vegne av foretaksgruppen, dvs. fra 15. september 2016.

Denne rapporten utgjør en foreløpig redegjørelse og endelig rapport skal foreligge i juni 2017. PwCs foreløpige hovedkonklusjoner fra undersøkelsen er:

1. Sykehuspartner har ikke tilstrekkelig kontroll på tilgangsstyring
2. Sykehuspartner har ikke tilstrekkelig sporbarhet på tilganger til helseopplysninger
3. Minst 34 personer tilknyttet ESN-avtalen har hatt mulighet til å få tilgang til helseopplysninger
4. Beslutning om tilganger knyttet til ESN-avtalen burde vært eskalert
5. ESN har så langt ikke kunnet dokumentere at det foreligger databehandleravtaler med underleverandører
6. Sentrale informasjonssikkerhetsrisikoer knyttet til ESN-kontrakten er ikke blitt tilstrekkelig vurdert
7. Svakheter i metodikk for risikovurderinger og uklarheter i beskrivelsen av nivå for akseptabel risiko innenfor informasjonssikkerhet
8. Presentasjonen til styret i Helse Sør-Øst i sak 069-2016 vedrørende IKT-infrastrukturmodernisering var upresis og varsler om dette er ikke kommunisert til administrerende direktør i HSØ RHF.

2 Introduksjon

2.1 Bakgrunn

Styret i Helse Sør-Øst RHF (heretter HSØ RHF) besluttet 8. september 2016 (sak 069-2016) å inngå kontrakt med en ekstern partner for å gjennomføre IKT-infrastrukturmodernisering.

Sykehuspartner HF (heretter Sykehuspartner) fikk i foretaksmøte 15. september 2016 i oppdrag å legge til grunn RHF styresak 069-2016 for videre arbeid med modernisering av IKT-infrastrukturen og å inngå kontrakt med den eksterne partner som samlet hadde det mest fordelaktige tilbudet.

Sykehuspartner inngikk 14. oktober 2016 avtale med Hewlett-Packard Norge AS (heretter HPE) om infrastrukturdrift og infrastrukturmodernisering. Effektiv kontraktsdato ble satt til 1. november 2016. Kontrakten ble våren 2017 overført til Enterprise Services Norge AS (heretter: ESN og ESN-kontrakten). Selskapet DXC Technology er etablert gjennom en sammenslåing av Enterprise Services enheten i Hewlett-Packard og selskapet CSC.

iMod er programnavnet for gjennomføring av ESN-kontrakten og infrastrukturmoderniseringen i Sykehuspartner. Ved omtale av foretaksgruppen benyttes forkortelsen HSØ.

2.1.1 Infrastrukturmodernisering i Helse Sør-Øst

HSØ har et stort digitalt utviklingsbehov og moderniseringen av IKT-infrastruktur er en forutsetning for å tilby bedre løsninger og tjenester for helsepersonell og pasienter. Arbeidet med infrastruktur-modernisering har pågått delvis fragmentert i flere år. ESN-kontrakten og iMod-programmet representerer en helhetlig tilnærming til å modernisere infrastrukturen slik at den kan understøtte øvrig modernisering i regi av programmet Digital fornying.

Deler av HSØs IKT-infrastruktur er utdatert og gjør det vanskelig å etterleve krav til informasjonssikkerhet. Systemer for sporing og logging er mangelfulle, pasientinformasjon og helseopplysninger er tilgjengelige for utvalgt driftspersonell i infrastrukturdrift, og deler av infrastrukturen er på et versjonsnivå som innebærer risiko for informasjonssikkerheten. Et sentralt formål med iMod er å rette opp i disse svakhetene.

2.1.2 Leverandørmarkedet og IKT-tjenesteutsetting

De fire helseregionene i Norge har om lag 2500 dedikerte IKT-medarbeidere, hvorav om lag 1300 medarbeidere er ansatt i HSØ.[1] Alle helseforetak har stor avhengighet til leverandører av IKT programvare, maskinvare og medisinteknisk utstyr. Leverandørene har en sentral rolle i å tilpasse og innføre nye løsninger, i løpende service og vedlikehold, samt i bistand til drift og forvaltning. Helseforetakene og IKT-selskapene i de fire helseregionene må gi og styre nødvendige tilganger til personell fra leverandørene slik at nødvendige oppgaver kan utføres. Oppgavene er bl.a. knyttet til å redusere risiko for driftsavbrudd og opprettholde garantier.

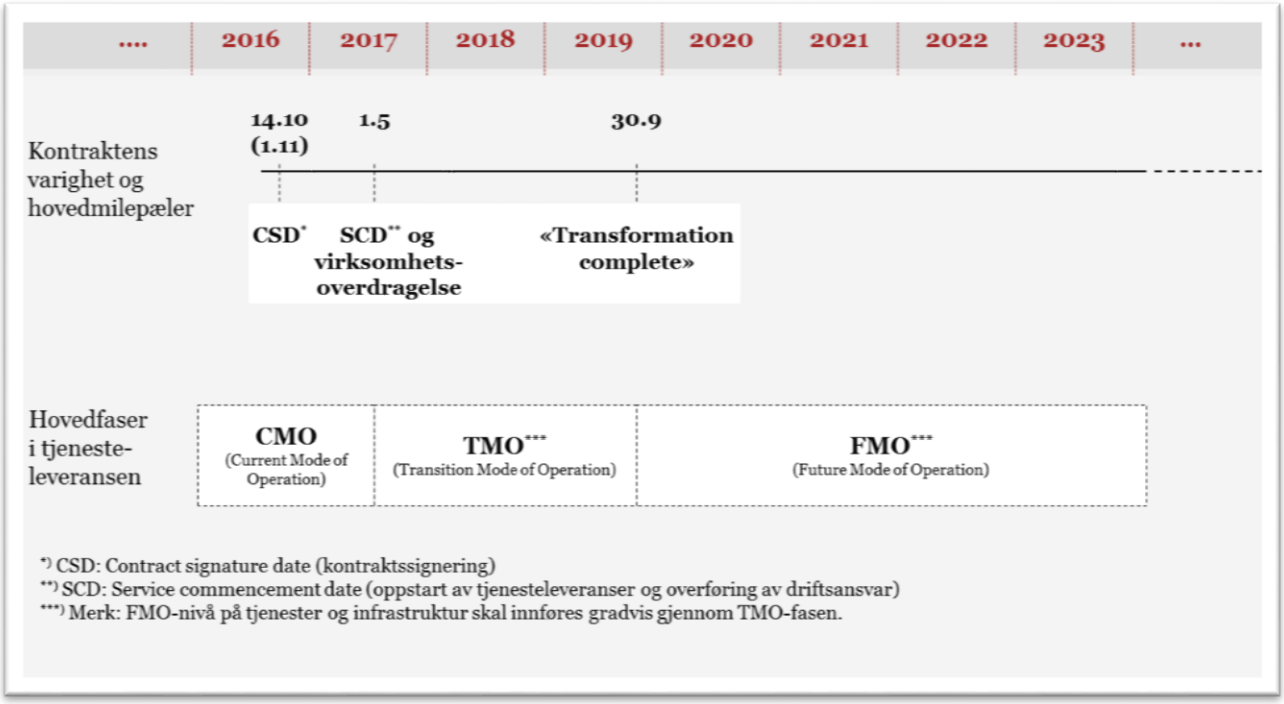
Utfordringer knyttet til kapasitet, kompetanse og kostnader har ført til at mange virksomheter i privat og offentlig sektor har tjenesteutsatt deler av IKT-funksjonen de siste årene. Dette gjelder særlig løsninger og oppgaver knyttet til infrastruktur, datasenter, nettverk og sluttbrukerløsninger (for eksempel PC, kontorstøtteapplikasjoner og service desk). Infrastruktur, nettverk og sluttbrukerløsninger er kritisk for enhver virksomhets operasjon, men mange virksomheter vurderer at det ikke er en del av kjernevirksomheten og at det krever for mye ressurser å forvalte og

[1] Direktoratet for e-helse

vedlikeholde grunnleggende infrastruktur. Sykehuspartners avtale med ESN representerer den første vesentlige IKT-tjenesteutsettingen i spesialisthelsetjenesten.

2.1.3 ESN-avtalens omfang og sentrale milepæler

ESN-avtalen, med effektiv kontraktsdato 1. november 2016, innebærer at driftsansvaret for IKT-infrastruktur overføres fra Sykehuspartner til ESN, inkludert virksomhetsoverdragelse av personell, samt en modernisering og standardisering av foretaksgruppens samlede IKT-infrastruktur. ESN-avtalen omfatter løsninger og tjenesteleveranser innen sluttbruker, telefoni, datasenter, nettverk, samt tjenester knyttet til bl.a. service management og sikkerhet. Figuren under illustrerer ESN-kontraktens varighet og sentrale faser og milepæler.



Figur 1 - ESN-avtalen, sentrale faser og milepæler

ESN-kontrakten inneholder en rekke krav knyttet til informasjonssikkerhet som skal oppfylles av leverandør. Faktisk fremdrift i tjenesteleveransene (jf. figuren over) betinger bl.a. at Security Board, på vegne av helseforetakene, og eventuelt HSØ RHF, godkjenner risikovurderinger knyttet til informasjonssikkerhet. I forbindelse med virksomhetsoverdragelsen (SCD) er det etablert en «operational readiness review» og et antall kriterier som skal oppfylles før virksomhetsoverdragelsen kan finnes sted.

2.2 PwCs oppdrag

PwC er HSØs revisor og ble 4. mai 2017 engasjert av administrerende direktør i HSØ RHF til å utføre et tilleggsoppdrag knyttet til påstander om at eksterne tilganger til HSØ IKT-infrastruktur kan ha gitt tilgang til sensitive personopplysninger, herunder helseopplysninger.

PwC skal gi en foreløpig redegjørelse i HSØ RHF sitt styremøte 24. mai 2017. Redegjørelsen skal omfatte:

- Status i gjennomføringen av programmet
- Vurdere kontrollregime knyttet til oppfyllelse av krav til informasjonssikkerhet, spesifikt:

  - Fakta om tilganger som er gitt, om de er gitt etter gjeldende rutiner, om det anses forsvarlig at disse tilgangene er gitt og om rutinene er forsvarlige
  - Undersøke eventuelt misbruk av tilganger og om personsensitive data har kommet på avveie
- Vurdering av systemet for gjennomføring av risikovurderinger knyttet til informasjonssikkerhet
- Om HSØ RHF har fått tilstrekkelig informasjon om risiko og gjennomføringen av programmet vedr. informasjonssikkerhet
- Andre relevante forhold

I endelig rapport, juni 2017, skal PwC:

- Vurdere styringsmodell, fullmakter, ansvar og roller som er etablert i programmet
- Evaluere hvorvidt programmet i Sykehuspartner HF er satt opp og styrt på en hensiktsmessig måte for å gjennomføre oppgavene gitt i foretaksmøte 15. september 2016
- Vurdere ESN-avtalen mhp. ivaretagelse av informasjonssikkerhet og sikring av personsensitiv informasjon

PwCs undersøkelser og vurderinger er knyttet til perioden fra Sykehuspartner HF fikk oppdraget med å inngå kontrakt og gjennomføre programmet på vegne av foretaksgruppen, dvs. fra 15. september 2016.

2.3 Grunnlag for foreløpig redegjørelse

Tabellen under beskriver grunnlaget for PwCs foreløpige redegjørelse.

Periode	PwC startet oppdraget 4. mai 2017
Dokumentasjon	PwC har forespurt relevant dokumentasjon og mottatt nærmere 300 dokumenter. Dokumentene har blitt OCR-behandlet* av PwC for å muliggjøre søk i skannede dokumenter. I tillegg har PwC mottatt 3 dokumenter fra HSØ RHF, opprinnelig sendt fra medarbeidere i Sykehuspartner, som uttrykker bekymringer knyttet til iMod-programmet. Dokumentene er oversendt HSØ RHF etter 4. mai 2017.
Data	PwC har gjennomført søk i data hentet ut fra Sykehuspartners sentraliserte logghåndteringsplattform**, herunder logger fra Active Directory, Domenekontrollere, og Leverandørportalen. Analysene er gjort med grunnlag i loggdata fra tidsrommet 02.02.17 – 19.05.17. Vi har i tillegg mottatt personellister fra Sykehuspartner og fra HPE/DXC Technology.
Begrensninger i datagrunnlaget	Datagrunnlaget PwC har hatt til disposisjon er ufullstendig. Sykehuspartners sentrale logginnsamlingssystem inneholder i hovedsak loggdata fra SIKT og Oslo universitetssykehus (OUS), men mangler data fra eksempelvis Akershus universitetssykehus (AHUS). Datagrunnlaget gir ikke mulighet til å vurdere hvorvidt konfidensialiteten eller integriteten til sensitive personopplysninger i ulike systemer har blitt kompromittert. Mangelen på sporbarhet medfører at PwC ikke kan verifisere hvorvidt helseopplysninger har havnet på avveie som et resultat av uhell eller uønskede villede handlinger.
Intervjuer	PwC har i innledende fase gjennomført møter med et utvalg nøkkelpersoner. Vi har i tillegg gjennomført 9 intervjuer med ansatte i Sykehuspartner og HSØ RHF.

Sentrale forbehold	Vi bygger våre konklusjoner utelukkende på dokumenter vi har fått tilgang til og informasjon framkommet gjennom intervjuer. Vi kan ikke utelukke at vi ikke har blitt gjort kjent med forhold som kunne ha påvirket våre konklusjoner. Vi har gjennomført helt eller delvis kontradiksjon med 5 personer som vi anser som berørt av innhold i rapporten. 2 ytterligere berørte har ikke vært tilgjengelig for kontradiksjon. Det må derfor tas forbehold om at dette kan påvirke det endelige innholdet i rapporten.

**) OCR: Optical character recognition, en metode for å konvertere bildetegn til maskinlesbar tekst*

***) Splunk: Et kommersielt Security Incident and Event Management (SIEM) system*

3 Status i gjennomføringen av programmet

Den planlagte virksomhetsoverdragelsen mellom Sykehuspartner og ESN skulle iht. kontrakt vært utført 1. mai 2017, men er foreløpig utsatt. Hovedårsakene til utsettelsen var at sentrale verktøy for service management ikke var på plass, manglende morselskapsgaranti, utestående problemstillinger knyttet til informasjonssikkerhet, samt ikke oppfylte kriterier i «operational readiness review».

4 Kontrollregime knyttet til oppfyllelse av krav til informasjonssikkerhet

4.1 Sykehuspartner har ikke tilstrekkelig kontroll på tilgangsstyring

Faktiske forhold lagt til grunn

PwC har innhentet oversikt fra Sykehuspartner og ESN over hvilke brukere som har blitt opprettet og hvilke tilganger (rettigheter) de har fått. Listene PwC har mottatt fra de to partene samsvarer ikke.

Det finnes ingen sentral oversikt over hvilke tilganger som er gitt. Det har vært nødvendig å gjennomføre omfattende søk og analyser for å avdekke hvilke personer, brukerkontoer og tilganger som har vært tilknyttet kontrakten. I tillegg er det usikkert hvorvidt oversikten vi nå besitter er fullstendig gitt begrensningene i datagrunnlaget for gjennomførte søk og analyser.

PwCs analyser av brukere viser at flere har fått høyere rettigheter enn de har hatt behov for. Av de 34 brukerne er det 7 som har benyttet seg av disse (jf. 4.3).

PwC har foreløpig identifisert én bruker som har forsøkt å aksessere HSØs systemer utenfor tidsperioden for vedkommendes oppdrag.

PwCs vurdering

Per 23. mai 2017 kan ikke PwC bekrefte at vi har en fullstendig oversikt over hvilke brukere som er knyttet til kontrakten. PwC har siden 4. mai mottatt flere lister som skal gi oversikt over brukere, men antallet brukere har variert i de ulike versjonene. Mangelen på oversikt over antall brukere med rettigheter som kan medføre tilgang til helseopplysninger, kombinert med svake kontrollrutiner, øker risikoen for uautorisert tilgang. På bakgrunn av våre foreløpige undersøkelser vurderer PwC derfor Sykehuspartners tilgangsstyring som utilstrekkelig.

4.2 Sykehuspartner har ikke tilstrekkelig sporbarhet på tilganger til helseopplysninger

Faktiske forhold lagt til grunn

Løsningen Leverandørportalen er oppgitt som et av tiltakene som skal sikre sporbarhet på tilgang til IKT-systemene fra eksterne brukere. Leverandørportalen er en SSL-VPN-løsning som må benyttes for alle som ikke benytter klienter utlevert av Sykehuspartner (såkalte SIKT-klienter). Dette skal sikre tilstrekkelig logging og monitorering av aktiviteten til eksterne brukere. Samtidig skal løsningen sikre at informasjon fra Sykehuspartner sin infrastruktur ikke kan hentes ut gjennom denne tilkoblingen.

PwCs vurdering

Tildelingen av brukere med lokale administratorrettigheter, kombinert med begrenset sporbarhet, gir mulighet for personell å aksessere systemer som inneholder eller behandler helseopplysninger. Bruk av Leverandørportalen hever terskelen for å urettmessig aksessere helseopplysninger, men vår vurdering er at det vil være svært krevende å utelukke at helseopplysninger er kommet på avveie. Begrensningen i mulighet til å hente ut informasjon gjennom leverandørportalen er også vurdert som

en utilstrekkelig sikkerhetsmekanisme for brukere som har lokal administratortilgang på servere i HSØs IKT-infrastruktur.

Et eksempel på utfordringene med dette er fra våre undersøkelser av aktiviteten til en konkret bruker. Denne brukeren var tildelt utvidete administratorrettigheter i forbindelse av vedkommendes deltagelse i T1-P19 RTPA (Scanning), en aktivitet som foregikk i tidsperioden 23.03.17 til 11.04.17. Basert på analyser av logger fra leverandørportalen fremkommer det at brukeren logget seg på 21.04.17 fra en IP-adresse tilknyttet Hewlett-Packard i Tyskland. Dette var i en periode da brukeren hadde utvidete administratortilganger som ga vedkommende lokale administratorrettigheter, og dette foregikk fra en utenlandsk lokasjon etter at aktiviteten T1-P19 RTPA var avsluttet. For å få klarhet i dette har PwC gjennomført tre aktiviteter:

- Innhentet redegjørelse fra ESN for hvorfor brukeren var tilkoblet på dette tidspunktet
- Etterspurt audit-logger fra en av de aktuelle serverne brukeren kan ha aksessert
- Innhentet ytterligere uttrekk fra logger fra domenekontrollere (Windows Security Events)

I denne konkrete undersøkelsen oppgir ESN at brukeren kun gjennomførte et forsøk på innlogging, men aldri fullførte det, og at hensikten var å kontrollere at fjernaksessløsningen fungerte. PwC har hverken klart å bekrefte eller avkrefte denne påstanden gjennom loggene fra leverandørportalen. Det finnes heller ikke audit-logger for den aktuelle serveren fra tidsperioden, noe som gjør det krevende å vite hva brukeren faktisk har foretatt seg.

4.3 Minst 34 personer tilknyttet ESN-avtalen har hatt mulighet til å få tilgang til helseopplysninger

Faktiske forhold lagt til grunn og metodikk

PwC har gjennom analyser av uttrekk fra Active Directory (AD), sammenstilt med en oversikt fra ESN, identifisert totalt 193 brukere i HSØ sine systemer som er tilknyttet ESN-kontrakten. Av disse har vi gjennomgått akkumulerte tilganger og rettigheter siden brukerne ble opprettet. Disse har vi kryssjekket mot en oversikt over tilganger som kan gi lokal administratortilgang til en eller flere servere knyttet til systemene Dips, Metavision, Neonatal, Partus, Imatis og Kurve.

I vår oversikt har vi inkludert totalt 811 servere tilknyttet disse systemene. Dette er servere som ifølge opplysninger fra Sykehuspartner skal ha lagret helseopplysninger. Denne listen over servere er begrenset til de overnevnte systemene, og det er trolig et større antall andre servere som lagrer eller prosesserer helseopplysninger knyttet til andre systemer eller fagapplikasjoner.

Foreløpige analyser viser at av de 34 brukerne er det 7 som har aksessert én eller flere av de 811 serverne.

PwCs vurdering

Ut fra disse analysene har vi identifisert 34 personer som er gitt brukere med tilganger av en slik karakter at de har eller vil kunne tildele seg eller andre brukere lokale administratorrettigheter på en eller flere av disse serverne. Dette tallet er konservativt fordi vi har ekskludert brukere som har hatt utvidede rettigheter, uten at vi har klart å bekrefte tilgang til en eller flere av de 811 overnevnte serverne med tilganger på et nivå som gir lokale administratorrettigheter. PwC vurderer at det ikke er mulig å forhindre at brukere med lokale administratortilganger på servere har tilgang til helseopplysninger som er lagret på disse serverne. I tillegg er det stor sannsynlighet for at disse rettighetene også har gitt tilgang til eksempelvis brukere i HSØ sine hjemmeområder og e-post.

4.4 Beslutning om tilganger knyttet til ESN-avtalen burde vært eskalert

Faktiske forhold lagt til grunn

I behandlingen av «Impact Assessment for Privacy Disadvantage», som kan forstås som en risikovurdering rettet mot personvern, levert av HPE i iMod Security Board 24.03.17, ble det identifisert flere røde risikoer. Disse tilgangene mente HPE var nødvendige for å gjennomføre aktivitetene T2-P19 Knowledge Transfer og RTPA. I denne vurderingen fremkommer det også at flere av disse tilgangene vil medføre at personell tilknyttet ESN-kontrakten vil kunne få tilgang til helseopplysninger. Dette inkluderer også en oversikt over 14 navngitte personer knyttet til aktiviteten T2-P19 Knowledge Transfer Offsite som etter oversikten skal foregå i Bulgaria. Det er også skissert en rekke tiltak knyttet til dette, uten at det fremkommer fra dokumentasjonen om dette er identifiserte eller implementerte tiltak.

I referatet fra samme møtet i iMod Security Board fremkommer det at risikovurderingene er godkjent, med forbehold om at:

- Leverandørportalen skal benyttes
- Sykehuspartner skal gi ut tilganger
- De foreskrevne tiltakene skal implementeres

I dokumentene som foreligger er det ikke beskrevet noen vurdering av risiko etter tiltak. I intervju oppgir administrerende direktør Sykehuspartner at hun ikke har blitt forelagt noen informasjonssikkerhetsrisikoer som er utenfor akseptkriteriene.

PwCs vurdering

PwC vurderer at risikoen knyttet til tildelinger av tilganger i forbindelse med T2-P19 burde vært eskalert til administrerende direktør Sykehuspartner. Det fremkommer ikke om det er nåværende- eller restrisiko som danner grunnlaget for en eventuell eskalering. Videre er det heller ikke dokumentert at restrisiko etter tiltak er innenfor risikoaksept. I tillegg vurderer HPE at tilgangene de ber om vil medføre tilgang til helseopplysninger. PwC vurderer dette som et forhold som ytterligere tilsier at risikoen burde vært eskalert til administrerende direktør Sykehuspartner.

4.5 ESN har så langt ikke kunnet dokumentere at det foreligger databehandleravtaler med underleverandører

Faktiske forhold lagt til grunn

ESN/HPEs rettsgrunnlag for behandling av personopplysninger er sikret ved inngåelse av databehandleravtale med Sykehuspartner. Gjennom databehandleravtalen sikrer Sykehuspartner at hovedleverandør:

- bare behandler personopplysninger i tråd med mandatet i kontrakten
- oppfyller lovens og kontraktens krav til informasjonssikkerhet

PwC har per 23. mai 2017 ikke mottatt databehandleravtaler mellom ESN/HPE og deres underleverandører. Merk at personell fra HPE er ansatt i ulike juridiske enheter. Personopplysninger kan i utgangspunktet ikke overføres fra ESN/HPE til underleverandører uten at det er inngått databehandleravtaler mellom selskapene som oppfyller lovens krav. Kravet til at hovedleverandør inngår databehandleravtaler med sine underleverandører framgår av avtalens Appendix 2, Annex A, punkt 6.1.1.

PwC har, gjennom Sykehuspartner, etterspurt disse avtalene og dessuten spurt hvilket selskap de omhandlede bulgarske IT-medarbeiderne er ansatt i. Sykehuspartner har hentet svaret fra signerte "Confidentiality Agreements". Her opplyses at de 31 brukerne som fikk sine tilganger stengt i perioden 27.4 - 2.5 er/var ansatt i HPE, hvorav 28 har bulgarsk statsborgerskap og 3 har ulike andre europeiske statsborgerskap. Dette er ikke tilstrekkelig til å fastslå hvilken konkret juridisk enhet de har vært ansatt i.

PwCs vurdering

Det foreligger risiko for at ansatte hos/representanter for ESN/HPEs underleverandørene har hatt tilgang til- og mulighet for å behandle personopplysninger uten at de har hatt rettsgrunnlag for dette, herunder garantert tilstrekkelig informasjonssikkerhet og formålsrettet behandling. ESN/HPE har dermed eventuelt ikke oppfylt sine kontraktsforpliktelser vedrørende dette punktet.

5 Systemet for gjennomføring av risikovurderinger knyttet til informasjonssikkerhet

5.1 Sentrale informasjonssikkerhetsrisikoer knyttet til ESN-kontrakten er ikke blitt tilstrekkelig vurdert

Faktiske forhold lagt til grunn

Landrisikovurderingen i forbindelse med tilgang fra Bulgaria, behandlet i ekstraordinært RSV-møte 10. mars 2017, konkluderte med at svakheter i infrastrukturen fører til uakseptabel risiko før tiltak. Eksplisitte vurderinger av tiltakenes risikoreduserende effekt fremkommer ikke. Landrisikovurderingen ble tilsluttet av 6 av 11 stemmeberettigede i RSV, 3 blanke og 2 ikke tilsluttet.

I etterkant av ekstraordinært RSV møte blir Administrerende Direktør i Sykehuspartner gitt følgende fullmakt fra helseforetakene (signert av Sykehuspartner, 16. mars 2017):

«Administrerende direktør i Sykehuspartner HF gis herved fullmakt til å opptre på vegne av de undertegnede i gjennomføringen av avtale med HPE innenfor informasjonssikkerhetsområdet.» Fullmakten innebærer også: *«…iMod Security Board kan akseptere risiko som påvirker databehandlingsansvarlige så fremt at risikoen vurderes som akseptabel.»*

iMod Security Board 24. mars 2017 behandlet risikovurderinger i forbindelse med tilgang til CMO fra Bulgaria (ref. "Risk assessment Access to CMO from Bulgaria - Availability" og "Bulgaria CMO Access for Knowledge Transfer"). iMod Security Board 11. april 2017 behandlet risikovurdering i forbindelse med tilgang til TMO fra Bulgaria (ref. «Privacy disadvantage and risk assessment - Access to TMO from Bulgaria»). Alle risikovurderingene viser flere risikoer utenfor regionalt akseptnivå (før tiltak), men blir vedtatt med forutsetninger om at risikoreduserende tiltak blir gjennomført.

PwCs vurdering

Den gjennomførte landrisikovurderingen har avdekket at kjente svakheter i infrastrukturen medfører høyere risiko i forbindelse med de tilgangene som må gis ved gjennomføring av oppgaver som skal utføres fra Bulgaria. Det fremstår ikke av etterfølgende risikovurderinger behandlet i iMod Security Board at disse svakhetene er tilstrekkelig hensynstatt. Dette fører til at det vi oppfatter er vesentlige svakheter i IKT-infrastrukturen ikke legges til grunn for vurdering av tiltak eller eskalering av risiko.

5.2 Svakheter i metodikk for risikovurderinger og uklarheter i beskrivelsen av nivå for akseptabel risiko innenfor informasjonssikkerhet

Faktiske forhold lagt til grunn

Fullmakten gitt av helseforetakene til Administrerende Direktør i Sykehuspartner refererer til regionalt akseptnivå for risiko. HSØ angir regionalt akseptnivå på følgende måte:

"Regionalt akseptabelt risikonivå, er definert ut fra vår 4x4 matrise for risikovurderinger. Denne er definert som følger:

- *Risiko med verdi 1-5 (1-4) er innenfor akseptnivå (Grønn)*
- *Risiko med nivå 6-9 (6, 8 og 9) er utenfor akseptnivå (Gult), og det skal utarbeides tiltak for å lukke sårbarheten.*
- *Risiko med nivå (12 og 16) er utenfor akseptnivå (Rødt), og det skal utarbeides tiltak for å lukke sårbarheten. Ofte vil disse tiltakene være krevd lukket før implementering."*

I mal for risikovurderinger benyttet av iMod Security Board refereres det til HSØs styringssystem for informasjonssikkerhet og videre til dokumentet *«Risikovurderinger – bakgrunn for sannsynlighet og konsekvens» (Regionalt sikkerhetsfaglig råd, 6/12-2016)* for kriterier for vurdering av sannsynlighet og konsekvenser. I dokumentet er akseptnivåene gjengitt på følgende måte:

1.6. Risikomatrise

Risikomatrisen viser hvordan risiko beregnes

Konsekvens / Sannsynlighet	4 Katastrofal konsekvens	3 Stor konsekvens	2 Moderat konsekvens	1 Liten konsekvens
4 Svært høy sannsynlighet	Høy	Høy	Medium	Medium
3 Høy sannsynlighet	Høy	Høy	Medium	Medium
2 Moderat sannsynlighet	Medium	Medium	Lav	Lav
1 Lav sannsynlighet	Medium	Medium	Lav	Lav

1.7. Akseptabelt risikonivå

Med utgangspunkt i kriterier for konsekvens og sannsynlighet beskrevet foran kan akseptabelt risikonivå angis som følger:

Akseptabel risiko settes til kombinasjonen katastrofal konsekvens/lav sannsynlighet eller moderat konsekvens/moderat sannsynlighet.

Det vil si at akseptabel risiko er enhver risiko som har produkt 6 eller lavere. For

Figur 2 – Akseptkriterier som beskrevet i HSØs styringssystem for informasjonssikkerhet

Det er avvik mellom de oppgitte regionale akseptnivåene og akseptnivåene i styringssystemet.

Styringssystemet for informasjonssikkerhet viser til konsekvensskalaer for Helsehjelpen, Forholdet til pasienten, Helsevesenet, Helseforetaket og Medarbeiderne. I risikovurderingene behandlet i iMod Security Board er risikoene vurdert i forhold til konsekvenser for konfidensialitet, integritet, tilgjengelighet og sporbarhet (KITS), men ikke vurdert opp mot konsekvenskategoriene i styringssystemet.

Det er ikke fremkommet at resultat av risikovurderinger er eskalert fra iMod Security Board til administrerende direktør i Sykehuspartner i henhold til fullmakt.

Det er ikke angitt om regionalt akseptnivå refererer til risikonivået før eller etter tiltak. I risikovurderingene er det ikke dokumentert vurderinger av restrisikonivå (dvs. hvilken risikoreduserende effekt de foreslåtte tiltakene forventes å ha). Da det fremstår som at iMod Security Board har vedtatt risikoer ut ifra restrisikonivå, er det vanskelig å kontrollere om det er vedtatt risikoer utenfor akseptnivå (dvs. risikoer som burde blitt eskalert).

Det er uklart om regionalt akseptnivå refererer til kriteriene for sannsynlighet og konsekvens som er gitt i HSØs styringssystem for informasjonssikkerhet, ref. dokumentet *«Risikovurderinger – bakgrunn for sannsynlighet og konsekvens»*. Det oppgitte risikonivået korresponderer ikke med dokumentets risikomatrise og dens fargeskalering. Konsekvenskriteriene i dokumentet er heller ikke brukt i risikovurderingene som er behandlet i iMod Security Board.

PwCs vurdering

Da det er vist til regionalt akseptnivå i fullmakten fra helseforetakene til Sykehuspartner og iMod Security Board, er det vesentlig at akseptnivået er klart beskrevet for å forstå hvilke risikoer iMod Security Board kan akseptere og hvilke risikoer de skal eskalere til administrerende direktør i Sykehuspartner.

Uklarheter knyttet til kriterier for risikoaksept og metodikk (bruk av konsekvensskalaer) fører til uklarheter for hvem som kan akseptere hvilke risikoer. Dette kan føre til at man ikke eskalerer risikoer som burde vært eskalert, og at systemet for vurdering av risiko ikke fungerer som et effektivt kontrollsystem.

6 Om Helse Sør-Øst RHF har fått tilstrekkelig informasjon om risiko og gjennomføringen av programmet vedr. informasjonssikkerhet

6.1 Presentasjonen til styret i Helse Sør-Øst i sak 069-2016 vedrørende IKT-infrastrukturmodernisering var upresis og varsler om dette er ikke kommunisert til administrerende direktør i HSØ RHF

Faktiske forhold som er lagt til grunn

ESN-kontrakten regulerer en tre-trinns prosess, henholdsvis nåværende operasjonsmodus (CMO), overføringsfasen (TMO) og fremtidig operasjonell drift på fornyet infrastruktur hos leverandør (FMO). I CMO-fasen er det behov for at leverandør får tilgang til nåværende infrastruktur hos Sykehuspartner blant annet for å gjennomføre aktiviteter knyttet til kunnskapsoverføring og kartlegging av infrastruktur.

Det følger av kontrakten at representanter for ESN skal gis tilgang for å kunne utøve nødvendige oppgaver i nåværende infrastruktur etter forutgående risikovurderinger. Tilstanden på infrastrukturen innebærer at enkelte av disse tilgangene også vil innebære muligheten for å få tilgang til pasientopplysninger.

I HSØ RHF styresak 069-2016 8. september 2016 ble det gitt en presentasjon hvor det bl.a. ble presentert følgende informasjon:

- *«Personell som drifter infrastruktur skal ikke ha tilgang til personsensitiv informasjon – egne sikkerhetsmekanismer for dette»*
- *«Ekstern partner vil ikke ha tilgang til pasientdata.»*

Det framgår ikke av presentasjonen hvilke faser i kontraktsforløpet disse kravene knytter seg til.

En representant for Sykehuspartner som var tilstede i styremøtet den 8. september 2016 uttrykte sin bekymring i en e-post 25. september 2016 til ledende ansatte i HSØ RHF. Vedkommende påpekte bl.a. følgende:

«Konkret gjelder det formuleringen i styresakens presentasjon foil #5 som fastslår at ekstern partner vil ikke ha tilgang til pasientdata. Dette er litt unyansert formulert/presentert og en forenkling av de sikkerhetskrav som er stilt i kontrakten og beskrevet i styresakens saksfremlegg. Kjernen i sikkerhetskravene er at i alle sammenheng skal lov og forskrifter skal oppfylles, og at det er satt spesielle krav knyttet til drift utenfor Norge og EU/EØS. Det er ikke kravstilt at ekstern partner ikke skal ha tilgang til pasientdata. Drift av infrastruktur medfører at driftspersonell får tilgang til pasientdata ved tjenestelig behov – slik er det for driftspersonell i Sykehuspartner i dag

og dette vil også gjelde for ekstern partner slik avtalen er formulert (uavhengig av om dette driftes fra Norge eller annet sted).»

Tilsvarende bekymring ble også adressert fra sikkerhetsleder i HSØ RHF i en e-post 18. oktober 2016 til en leder i HSØ RHF.

Sikkerhetsleder adresserte dette på nytt i en e-post 8. mars 2017 til samme leder samt en annen ledende ansatt i HSØ RHF. Hun påpekte dessuten følgende:

«De som drifter infrastrukturen drifter jo servere hvor pasientopplysninger beviselig ligger lagret.»

Våre undersøkelser har ikke kunnet fastslå at de ledende personene i HSØ RHF, som ble konfrontert med at informasjonen presentert for styret ikke var i tråd med de reelle forholdene i kontrakten, har bragt denne informasjonen videre til administrerende direktør i HSØ RHF.

I styremøte for Sykehuspartner 5. april 2017 fremmet ansattrepresentantene en protokolltilførsel vedr. sak om virksomhetsoverdragelse (sak 025-2017). Her framkommer følgende:

«Teknikere skal ikke ha tilgang til å logge seg på den enkelte fagapplikasjon, men kun tilgang til å logge seg på en server. Slik som systemet er satt opp i dag vil det allikevel være mulig for en tekniker å logge seg på en slik server og deretter hente ut informasjon fra denne. En slik informasjon vil i mange tilfeller kunne inneholde sensitive data, slik som: Pasient navn, personnummer, undersøkelse, diagnose med mer. Teknikere hos Helse Sør-Øst RHF sin eksterne partner vil få de samme tilgangene og dermed de samme mulighetene til å hente ut sensitiv informasjon.»

PwCs vurdering

Informasjonen presentert for styret i HSØ RHF gjenspeiler ikke det faktum at gjennomføringen av kontrakten vil kreve at risikoklarert driftspersonell vil få mulighet til å få tilgang til helseopplysninger. Selv om dette ble adressert i e-poster og mulig i samtaler til sentrale personer i HSØ RHF er det uheldig at Sykehuspartner ikke adresserte dette mer formelt i linjen, ved for eksempel et saksfremlegg for styret i Sykehuspartner. En ledende ansatt i HSØ RHF har hatt rollen som styreleder i Sykehuspartner og en annen ledende ansatt har vært medlem av iMod programstyre. Dette kan ha bidratt til at ansatte i Sykehuspartner har ansett at HSØ RHF har vært tilstrekkelig informert.

De ledende personene i HSØ RHF som ble konfrontert med informasjonen om avviket mellom det som var fremlagt for styret i HSØ RHF og reelle forhold burde umiddelbart ha adressert dette videre til administrerende direktør. For den ene ville dette innebære rapportering utenfor linjen. Det mener vi ville vært riktig i en sak som denne.