DET KONGELIGE
HELSE- OG OMSORGSDEPARTEMENT

Statsråden

Kontroll- og konstitusjonskomitéen
Stortinget
0026 OSLO

Deres ref	Vår ref	Dato
	vk/17/2133	1. juni 2017

Forespørsel fra kontroll- og konstitusjonskomitéen om nærmere opplysninger om sak om IKT-infrastruktur i Helse Sør-Øst

Jeg viser til brev av 9. mai i år fra Stortingets kontroll- og konstitusjonskomité om ovennevnte, og til mitt foreløpige svar på dette datert 15. mai i år.

Jeg mottok 24. mai redegjørelsen jeg hadde bedt om fra Helse Sør-Øst RHF om saken (vedlagt). Dette er en foreløpig redegjørelse utarbeidet av PwC etter en ekstern gjennomgang av Sykehuspartner HF og Helse Sør-Øst RHF sin håndtering av den planlagte tjenesteutsettingen knyttet til drift og modernisering av IKT-infrastruktur til Enterprise Services Norge AS (ESN)[1].

Den foreløpige redegjørelsen fra PwC viser at det har vært en svikt i Sykehuspartner HF sin gjennomføring av prosjektet. Sykehuspartner HF har ikke hatt en sentral oversikt over hvilke tilganger som har blitt gitt, og beslutninger om tilganger har etter PwC sin oppfatning delvis blitt gjort på et for lavt nivå i organisasjonen. PwC har gjennom sine analyser også kommet til at flere brukere har fått høyere rettigheter enn de har hatt behov for. PwC mener at tildeling av lokale administratorrettigheter, kombinert med begrenset sporbarhet, gir mulighet for personell å få tilgang til systemer som inneholder eller behandler helseopplysninger. De vurderer at leverandørportalens sikkerhetsmekanismer heller ikke er tilstrekkelige hvis en bruker er gitt lokal administratortilgang på servere i Helse Sør-Øst. PwC har også pekt på en mulig svakhet hos ESN, siden de så langt ikke har kunnet dokumentere at det foreligger databehandleravtaler med deres underleverandører.

PwC peker i sin redegjørelse på at Helse Sør-Øst sin IKT-infrastruktur er utdatert og gjør det vanskelig å etterleve krav til informasjonssikkerhet. Moderniseringen av IKT-infrastrukturen

[1] ESN ble kontraktpart våren 2017 etter en sammenslåing av Enterprise Services enheten i Hewlett-Packard og selskapet CSC til selskapet DXC Technology.

Postadresse: Postboks 8011 Dep 0030 Oslo
Kontoradresse: Teatergt. 9 Telefon* 22 24 90 90
Org no.: 983 887 406

er ifølge PwC en forutsetning for å kunne tilby bedre løsninger og tjenester for helsepersonell og pasienter. For en fullstendig oversikt over PwC sine vurderinger vil jeg vise til vedlagte redegjørelse datert 24. mai d.å. Jeg vil imidlertid kommentere deler av redegjørelsen senere i brevet knyttet til de konkrete spørsmålene fra Kontroll- og konstitusjonskomitéen i brev av 9. mai i år.

Bakgrunn

Spesialisthelsetjenesten er avhengig av private leverandører innenfor IKT-området, uavhengig av hvordan området er organisert. Dette gjelder blant annet bruk av programvare, maskinvare og medisinsk teknisk utstyr. Leverandørene har en sentral rolle i å tilpasse og innføre nye løsninger i sykehusene, gjennomføre nødvendig service og vedlikehold, og bidrar også i varierende grad med drift og forvaltning. Det er derfor et faktum at alle landets helseforetak og de regionale IKT-foretakene må gi og styre tilganger til personell fra leverandørene for å få utført nødvendige oppgaver.

Jeg har på bakgrunn av de forhold som har blitt avdekket når det gjelder tilgangsstyring i Sykehuspartner HF, og det faktum at hele spesialisthelsetjenesten har behov for å gi tilganger til private leverandører, sett behov for å samle kunnskap og initiere et utviklingsarbeid.

Jeg møtte den 29. mai i år alle styrene og administrativ ledelse i landets fire regionale helseforetak. På møtet satte jeg denne saken og tilgangskontroll på dagsorden. Jeg la vekt på betydningen av at de regionale helseforetakene lærer av hverandres erfaringer og gjennom dette utvikler bedre løsninger i fremtiden. Det er viktig at alle nå går gjennom egne systemer og rutiner knyttet til tilgangsstyring.

I forbindelse med saken i Helse Sør-Øst har jeg sett behov for å ta kontakt med Nasjonal sikkerhetsmyndighet (NSM). De har på et generelt grunnlag uttalt seg i media om denne saken. Departementet hadde et møte med ledelsen i NSM 16. mai i år. NSM orienterte om deres arbeid knyttet til sikkerhetsloven og informasjonssikkerhet generelt, og begge parter så behov for videre samarbeid på feltet. NSM pekte blant annet på at tjenesteutsetting generelt sett gir noen nye utfordringer knyttet til informasjonssikkerhet, og at dette er et forhold både de og ulike virksomheter bør få økt kunnskap om fremover. NSMs direktør Kjetil Nilsen hadde også en kronikk om dette i Dagens Næringsliv 16. mai i år, der han blant annet skriver:

> "Tjenesteutsetting av IKT-leveranser kan være en fornuftig avgjørelse. Det kan gi bedre sikkerhet og mer stabilitet og tilgjengelighet. Det kan gi lavere og mer forutsigbare kostnader og i større grad bidra til at virksomheten får konsentrert seg om egne kjerneområder. Samtidig må virksomheten være bevisst hvilke verdier som eksponeres ved tjenesteutsetting, og iverksette nødvendige tiltak. Behovet for konfidensialitet, integriet og tilgjengelighet bør særlig vektlegges i vurderingene, samt hvilke lover, krav og regler som gjelder nasjonalt og internasjonalt".

Jeg mener det er umulig å tenke seg en spesialisthelsetjeneste i dag uten at private leverandører er inne på en eller annen måte. Norske pasienter skal ha tilgang til moderne teknologi, røntgen, laboratorier, pasientjournalsystemer og velferdsteknologi. Det vil tjene pasientene å få tilgang til de teknologiske mulighetene som utvikles i det private markedet. Bruk av den best tilgjengelige teknologien er også avgjørende for å sikre både kvalitet og en kostnadseffektiv drift av helsetjenesten, og samtidig for å kunne møte fremtidige tjenestebehov. Vi må derfor klare å bruke internasjonale leverandører av teknologi på en god måte. Spørsmålet er derfor ikke om vi skal ha internasjonale leverandører, men hvordan vi gjør det på en god måte for å sikre hensynet til informasjonssikkerhet.

Jeg vil sikre at vi har en god og felles forståelse av hva som skal til for en trygg og riktig bruk av både nasjonale og internasjonale leverandører, enten det er bruk av ulik teknologi eller leveranse av drift av IKT-løsninger. Jeg vil derfor sette i gang et arbeid for å se på håndtering av informasjonssikkerhet ved bruk av private underleverandører i helse- og omsorgssektoren. Et element i dette er de utfordringer som knytter seg til bruk av internasjonale leverandører. Arbeidet skal ledes av Direktoratet for e-helse. De må sikre at de sentrale kompetansemiljøene blir trukket inn i arbeidet, og at fagorganisasjoner, tillitsvalgte og brukerorganisasjoner blir invitert til å komme med sine innspill. Behovet for å se på forholdet mellom helsetjenesten og sikkerhetsloven må også vurderes. Det er viktig at vi gjennom dette arbeidet settes bedre i stand til å håndtere de utfordringene vi er kjent med, og jeg ønsker derfor at det foreligger et resultat allerede 1. november inneværende år.

Jeg vil også gjøre oppmerksom på at Datatilsynet i likelydende brev av 26. mai til alle databehandlingsansvarlige i Helse Sør-Øst har bedt det enkelte foretak om å sende inn følgende dokumentasjon:

1. Risikovurderingen samt redegjørelse for akseptanse av restrisiko jf. personopplysningsforskriften § 2-4 jf. pasientjournalloven § 22 som ble lagt til grunn da det ble besluttet at drift og leveranse av IKT-infrastrukturen i helseregionen skulle tjenesteutsettes.
2. Risikovurderingene samt redegjørelse for akseptanse av restrisiko som ble lagt til grunn da det ble besluttet å legge disse tjenestene til Bulgaria.
3. En oversikt for hvor mange eksterne leverandører som har tilgang til sykehusenes informasjonssystem, hvilke land leverandørene har tilgang fra, hvilke typer tilganger de har til hvilke systemer og til hvilke personopplysninger (omfang, sensitivitet), samt formålet med tilgangene.

Frist for redegjørelsene er satt til 15. juni 2017.

Før jeg utdyper svarene på de konkrete spørsmålene komiteen stiller ønsker jeg kort å redegjøre generelt for det overordnede regelverket vedrørende de regionale helseforetakenes rettslige ansvar.

Det er presisert i spesialisthelsetjenesteloven § 2-1 a at de regionale helseforetakenes ansvar innebærer en plikt til å planlegge, gjennomføre, evaluere og korrigere virksomheten slik at tjenestenes omfang og innhold er i samsvar med krav fastsatt i lov eller forskrift. Tjenestene kan ytes av de regionale helseforetakene selv, eller ved at de inngår avtale med andre tjenesteytere.

Selv om deler av tjenesten er organisert som selvstendige rettssubjekter, beholder imidlertid det regionale helseforetaket det overordnede ansvaret for den virksomhet som drives av helseforetaket eller av andre underliggende tjenesteytere, herunder et kontroll og tilsynsansvar. Det følger av helseforetaksloven § 28 første ledd at "forvaltningen av foretaket hører under styret som har ansvar for en tilfredsstillende organisering av foretakets samlede virksomhet". Det er presisert i § 28 tredje ledd at for regionale helseforetak omfatter styrets plikter også helseforetak som foretaket eier. Forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten trådte i kraft 1. januar 2017. Forskriften erstatter og viderefører forskrift om internkontroll i helse- og omsorgstjenesten. I forskriften er det presisert at det er ledelsen som har ansvaret for at det etableres og gjennomføres systematisk styring av virksomhetens aktiviteter, herunder nødvendig risikovurdering og at medarbeiderne i virksomheten medvirker til dette. Virksomheten skal være forsvarlig i alle faser (planlegging, gjennomføring, evaluering, korrigering).

Det regionale helseforetaket har dermed det overordnede ansvaret for å sørge for systematisk styring av virksomhetens aktiviteter slik at informasjonssikkerhet og håndtering av personsensitive data i IKT-infrastrukturen ivaretas i regionen. Det er det enkelte helseforetak som etter loven er databehandlingsansvarlig og gjennom dette har et eget ansvar for informasjonssikkerheten.

Kontroll- og konstitusjonskomiteen ba i sitt brev av 9. mai i år om svar på følgende:

Spørsmål 1. Kan statsråden redegjøre for denne saken og samtidig redegjøre for når departementet har blitt informert om ulike deler av sakskomplekset underveis?

Mitt svar i brev av 15. mai d.å.:
"Jeg oppfatter at kontroll- og konstitusjonskomiteen er opptatt av tilganger for eksterne IKT-ansatte i forbindelse med planleggingen av overføring av ansvaret for driften av IKT-infrastrukturen, og hvorvidt disse tilgangene har gitt innsyn i personsensitive data. Dette er de samme forholdene som også media har vært opptatt av. Jeg opplever at jeg ikke har fått fullstendig informasjon om dette fra Helse Sør-Øst RHF, og har derfor som nevnt ovenfor, bedt Helse Sør-Øst RHF om en redegjørelse.

Den første faktakunnskap som har blitt gitt departementet knyttet til tilganger i planleggingen av overføringen av driftsansvaret til HPE kom fra Helse Sør-Øst RHF i forbindelse med departementets sluttføring av svar på spørsmål til skriftlig besvarelse nr 969 (2017) fra representanten Sverre Myrli. Dette var den informasjonen som ble gitt departementet den 27. april i år, og som nå er alminnelig kjent: "De ansatte i HPE som i dag har fått tilgang til vår IKT-infrastruktur har fått denne gjennom den såkalte leverandørportalen på lik linje med andre leverandører. Leverandørportalen har egne sikkerhetsmekanismer". Departementet oppfattet ikke at HPE-ansatte med dette hadde fått tilgang til personsensitive data. Vi oppfattet da at tilgangen gjennom leverandørportalen beskyttet personsensitive data gjennom de nevnte sikkerhetsmekanismene i leverandørportalen. Disse sikkerhetsmekanismene ble også beskrevet i svaret til representanten Myrli. Jeg vil igjen minne om at svaret som ble sendt til representanten Myrli var knyttet til den planlagte situasjonen etter at HPE har overtatt driftsansvar. Jeg hadde derfor på det tidspunktet ikke kunnskap om at det hadde blitt gitt eksterne tilganger som kunne gi mulighet til å tilegne seg personsensitive data under planleggingen av overføringen.

Representanten Micaelsen har i sitt spørsmål til skriftlig besvarelse nr. 1064 (2017) i tillegg spurt om hvilken informasjon jeg hadde fått da jeg møtte i Stortingets spontanspørretime 3. mai i år. Departementet mottok 2. mai en orientering fra administrerende direktør i Helse Sør-Øst RHF. Vi hadde tidligere samme dag fått en intervjuforespørsel fra NRK som beskrev tilgang til personsensitive data. I informasjonen fra Helse Sør-Øst RHF 2. mai gikk det frem at det var gitt midlertidige tilganger for en begrenset periode for 12 ansatte i HPE for opplæring. Disse tilgangene ble gitt via leverandørportalen og begrenset seg til en definert periode. Disse tilgangene ble ifølge informasjon fra Helse Sør-Øst RHF lukket 27. april da opplæring var gjennomført. Det ble også informert om at det var 16 personer fra HPE som hadde hatt midlertidig tilgang til infrastrukturen for kartlegging. Disse tilgangene ble ifølge Helse Sør-Øst RHF kun benyttet i Sykehuspartners lokaler og under kontroll av Sykehuspartner HF. Disse tilgangene var ifølge Helse Sør-Øst RHF også blitt lukket. Disse opplysningene ga jeg i mitt svar på spørsmål fra representanten Kjersti Toppe i den nevnte spontanspørretimen den 3. mai i år. Da var også saken til NRK publisert. Der mener NRK å kunne dokumentere tilgang av et helt annet omfang. Jeg kunne derfor ikke lenger være trygg på at den informasjonen jeg hadde fått fra Helse Sør-Øst RHF var korrekt. Derfor gjorde jeg det allerede i spontanspørretimen klart at jeg ville be Helse Sør-Øst RHF om en redegjørelse for saken, blant annet fordi jeg opplevde at det var et sprik mellom orienteringer fra Helse Sør-Øst RHF og medias fremstilling av saken. Denne redegjørelsen vil som nevnt ovenfor kunne bidra til å klargjøre flere av de spørsmålene som kontroll- og konstitusjonskomiteen reiser i sitt brev til meg, og jeg vil derfor komme tilbake til komiteen med et mer helhetlig og utfyllende svar."

Supplerende svar:
Jeg oppfatter at mitt svar i forrige brev er utfyllende mht. informasjon frem til 15. mai i år. Jeg har nå mottatt en mer omfattende orientering om saken gjennom den foreløpige redegjørelsen fra PwC. Redegjørelsen er vedlagt, og jeg vil kommentere elementer i denne i de neste spørsmålene.

Spørsmål 2. Kan statsråden nå gi en oversikt over hvem som har hatt tilgang på informasjon de ikke skulle ha hatt tilgang på?

Mitt svar i brev av 15. mai d.å.:
"Det vises til omtale over av den gjennomgangen som skal gjennomføres av PwC. Del I av dette oppdraget vil som nevnt utgjøre den redegjørelsen jeg har bedt om å få fra Helse Sør-Øst RHF, og som jeg vil motta 24. mai. I engasjementsbrevet (vedlagt) heter det blant annet:

"Del I av oppdraget skal blant annet belyse følgende forhold:

- *En oppdatert status på gjennomføringen av programmet i Sykehuspartner*
- *Programmets 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 i programmet knyttet til informasjonssikkerhet*
- *Om Helse Sør-Øst RHF har fått tilstrekkelig informasjon om risiko og gjennomføringen av programmet vedrørende informasjonssikkerhet*
- *Andre relevante forhold*

Basert på gjennomgangen skal det identifiseres tiltak som sikrer gjennomføring av programmet og/eller bidrar til å redusere risiko."

Av dette går det frem at jeg etter at denne redegjørelsen er gjennomført vil ha et langt bedre grunnlag for å gi et presist svar på spørsmålet. Jeg ber derfor om å få komme tilbake til dette etter at redegjørelsen foreligger."

Supplerende svar:
PwC sin redegjørelse viser at Sykehuspartner HF ikke har hatt noen sentral oversikt over tilganger som har blitt gitt, men deres analyser viser at minst 34 personer tilknyttet ESN-avtalen har hatt mulighet til å få tilgang til helseopplysninger. Videre viser deres analyser at det av disse 34 er 7 brukere som har "aksessert" én eller flere av de aktuelle 811 serverne som skal ha lagret helseopplysninger.

Når det gjelder tilgang på helseopplysninger, så skriver PwC følgende:

> "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."

PwC sin analyse har for øvrig identifisert totalt 193 brukere i systemene til Helse Sør-Øst som er tilknyttet ESN-kontrakten, men det er kun de ovenfor nevnte 34 som har hatt mulighet til å få tilgang til helseopplysninger.

Spørsmål 3. Har statsråden grunn til å tro at informasjon om norske pasienter kan ha kommet på avveie?

Mitt svar i brev av 15. mai d.å.:
"Jeg har ikke mottatt informasjon om at pasientopplysninger har kommet på avveie. Dette er et svært sentralt spørsmål som vil bli belyst i redegjørelsen fra Helse Sør-Øst RHF, jf. at PwC er bedt om å undersøke eventuelt misbruk av tilganger og om personsensitive data har kommet på avveie. Dette er også et spørsmål jeg vil komme tilbake til etter at redegjørelsen foreligger."

Supplerende svar:
Når det gjelder tilgang på helseopplysninger så sier PwC følgende (jf. også spørsmålet over):

"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."

Jeg oppfatter med dette at PwC ikke kan utelukke at noen kan ha skaffet seg tilgang til helseopplysninger. De bekrefter heller ikke at noen faktisk har brukt sin tilgang til å skaffe seg slike opplysninger urettmessig.

Spørsmål 4. Hva er departementets vurdering av skadeomfanget dersom pasientopplysninger har kommet på avveie, og hva er departementets vurdering av alvoret i denne saken?

Mitt svar i brev av 15. mai d.å.:
"Jeg har som nevnt ikke mottatt informasjon om at pasientopplysninger har kommet på avveie. Hvis redegjørelsen fra Helse Sør-Øst RHF viser at det har kommet pasientopplysninger på avveie, så er dette selvfølgelig alvorlig. Det er vanskelig for meg nå å

spekulere i et potensielt skadeomfang knyttet til at slike opplysninger skulle vise seg å være på avveie."

Supplerende svar:
Jeg viser her innledningsvis til mitt svar på spørsmål 3.

Det er alvorlig hvis pasientopplysninger kommer på avveie. Jeg har derfor på bakgrunn av denne saken i møte med landets regionale helseforetak 29. mai tatt et initiativ for å sikre at de umiddelbart retter sin oppmerksomhet på denne problemstillingen og de aktuelle forholdene rundt tilgangsstyring til eksterne leverandører. Jeg vil i tillegg gi et oppdrag til Direktoratet for e-helse der de blir bedt om å se på håndtering av informasjonssikkerhet ved bruk av private underleverandører i helse- og omsorgssektoren.

Spørsmål 5. Hva har statsråden gjort for å sikre seg om at denne saken ryddes opp i?

Mitt svar i brev av 15. mai d.å.:
"Jeg har bedt om en redegjørelse fra Helse Sør-Øst RHF. Denne redegjørelsen vil gi grunnlag for en bedre forståelse av fakta i saken, og gjennom det også gi meg et bedre grunnlag for å vurdere om jeg bør gjøre noen styringsmessige grep. Redegjørelsen vil dessuten gi Helse Sør-Øst RHF et bedre grunnlag for å vurdere om det er behov for ytterligere tiltak for å sikre informasjonssikkerheten i regionen.

Jeg vil ellers understreke at Helse Sør-Øst RHF har informert departementet om at de har lukket alle tilganger til IKT-infrastrukturen for ansatte i HPE knyttet til programmet for modernisering av IKT-infrastruktur."

Supplerende svar:
Utover mitt svar den 15. mai i år, så viser jeg til de to tiltakene jeg nevnte i foregående svar.

Når det gjelder den konkrete saken viser jeg også til det enstemmige vedtaket som ble gjort i styret for Helse Sør-Øst RHF i ekstraordinært styremøte 24. mai i år. Vedtaket er som følger:

> "Styret understreker behovet for at pasientene må føle seg trygge på at sensitive personopplysninger ivaretas på en trygg og sikker måte og dette innebærer at en modernisering av IKT-infrastrukturen er helt nødvendig.
>
> 1. Styret tar den foreløpige redegjørelsen fra PwC til etterretning.
>
> 2. Forutsetningen for infrastrukturmodernisering har vært at tilganger til sensitive personopplysninger ivaretas på en trygg og sikker måte, og styret konstaterer at dette ikke er ivaretatt.
>
> 3. Prosjektet, inkl virksomhetsoverdragelse og overdragelse av driftsansvar fra Sykehuspartner til ekstern leverandør, stilles i bero inntil videre.

4. Styret ber styreleder avholde foretaksmøte i Sykehuspartner HF som sikrer at prosjektet stilles i bero, og at følgende arbeid prioriteres for å belyse hvordan videre infrastrukturmodernisering kan sikres;
   - System for tilgangsstyring må gjennomgås, forsterkes og implementeres
   - Metodikk for risiko- og sårbarhetsanalyser knyttet til informasjonssikkerhet må gjennomgås, forsterkes og implementeres
   - Fornyede risiko- og sårbarhetsanalyser må gjennomføres og forankres med helseforetakene som databehandleransvarlige
   - Nødvendige endringer knyttet til leveranse og leveranseplaner i kontrakten som ivaretar IKT-informasjonssikkerhet på en trygg og sikker måte må utredes
   - Plan for styrking av styring, ledelse og gjennomføring av prosjektet må utarbeides.

5. Styret vil behandle saken igjen på et ekstraordinært styremøte i uke 26 når endelig rapport fra PwC og foreløpige resultater av utredningsarbeidet i punktet over foreligger. Som en del av dette vil også terminering måtte vurderes.

6. Styret ber administrerende direktør komme tilbake til styret med en utvidet orientering om hvordan pasientsikkerheten og personsensitiv informasjon håndteres i dagens situasjon."

Jeg har videre konstatert at det har skjedd endringer i ledelsen i Helse Sør-Øst RHF og at styret for Sykehuspartner HF ble skiftet ut i foretaksmøte 31. mai. I samme foretaksmøtet ble styret gitt et omfattende oppdrag både knyttet til å håndtere dagens driftssituasjon og å se på alternative gjennomføringsplaner for moderniseringen av IKT-infrastrukturen i Helse Sør-Øst. Det forutsettes at Sykehuspartner HF gjennomfører dette arbeidet med god involvering av ansatte og tillitsvalgte (se vedlagte protokoll fra foretaksmøtet i Sykehuspartner HF).
PwC arbeider videre med sin gjennomgang og vil levere en del 2 som er planlagt å bli behandlet i ekstraordinært styremøte i løpet av uke 26, altså siste uke i juni.

Jeg følger naturligvis med på den videre håndtering av denne saken i Helse Sør-Øst RHF.

Spørsmål 6. Er det riktig det som statsråden sa i Stortinget i interpellasjonsdebatten 10. november 2016 om at: "...personopplysninger ikke skal overføres til andre land ..."?

Mitt svar i brev av 15. mai d.å.:
"Interpellasjonsdebatten i Stortinget 10. november 2016 handlet om den fremtidige situasjonen etter at drift av IKT-infrastruktur var overført til en ekstern leverandør. Som tidligere opplyst i brevet har overføringen til HPE ennå ikke skjedd. De tilganger som har blitt gitt, og som ifølge Helse Sør-Øst RHF nå er lukket, har vært knyttet til en planleggings- og opplæringsfase. Mine svar i interpellasjonsdebatten omhandlet det sikkerhetsregimet som skal være på plass etter at driften er overført til ekstern leverandør.

Jeg vil igjen være klar på at jeg forventer at kun personell som har lovlig adgang skal ha tilgang til sensitive data. Dette er noe jeg vil ha spesiell oppmerksomhet på når gjennomgangen fra PwC foreligger (del I og del II)."

Supplerende svar: Utover mitt tidligere svar vil jeg vise til de opplysninger som fremkommer av redegjørelsen fra PwC. I redegjørelsen trekkes det frem som et eksempel en bruker som har hatt utvidete administratorrettigheter fra en IP-adresse tilknyttet Hewlett-Packard i Tyskland. I redegjørelsen omtales PwC sin undersøkelser rundt dette slik:

> "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."

Redegjørelsen omtaler også tilganger fra Bulgaria:

> "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 omtalen av disse tilgangene poengterer PwC at beslutningen om å tildele tilgangene burde vært forelagt administrerende direktør i Sykehuspartner HF.

Helse Sør-Øst RHF har orientert departementet om at alle pasientopplysninger vil være lagret i Norge. I arbeidet med å planlegge overføringen av ansvaret for drift til ekstern leverandør, har det imidlertid blitt gitt tilgang til IKT-infrastrukturen og serverne til IKT-ansatte utenfor Norge. Ifølge PwC har disse ikke hatt tilgang til selve pasientjournalsystemet.

I et møte med Helse Sør-Øst RHF 26. april i år ble det klargjort for meg at de begrensninger som ligger i at ekstern leverandør "ikke skal ha tilgang til helseopplysninger" ikke innebærer en absolutt sperre, men en kombinasjon av teknologiske, avtalemessige og juridiske sikkerhetsmekanismer som skulle hindre og eventuelt avdekke ureglementær tilgang. Jeg la i dette møtet vekt på at ledelsen måtte sikre seg at styret i Helse Sør-Øst RHF hadde tilsvarende informasjon, fordi jeg ble bekymret for at styret kunne ha oppfattet dette på samme måte som meg under sin behandling av saken tidligere. I brevet til Sverre Myrli 28. april ble det også gitt en beskrivelse av ulike sikkerhetsmekanismer, i tråd med den informasjonen jeg da hadde fått. Jeg vil understreke at dette omhandlet de fremtidige sikkerhetsmekanismene som skulle gjelde etter overtakelse. På dette tidspunktet var

departementet ikke kjent med at det hadde blitt gitt tilganger i planleggingsfasen. Denne informasjonen fikk departementet 2. mai gjennom henvendelse fra NRK og informasjon fra Helse Sør-Øst RHF.

Jeg vil avslutningsvis få understreke at jeg ser svært alvorlig på denne konkrete saken, noe som går frem av de tiltakene som er igangsatt. Jeg avventer nå den videre håndteringen av saken fra Helse Sør-Øst RHF sin side. Jeg er opptatt av de omdømmemessige sidene ved denne saken. Norske pasienter skal kunne ha en trygghet for at personsensitive opplysninger i helsetjenesten ikke kommer på avveie. Det er derfor viktig at både Helse Sør-Øst RHF og de øvrige regionale helseforetakene har en tilnærming til informasjonssikkerhet som bidrar til en slik trygghet. Mine beskrevne tiltak vil også kunne bidra til dette.

Med hilsen

Bent Høie

Vedlegg: Helse Sør-Øst RHF – foreløpig redegjørelse knyttet til IKT-tjenesteutsetting (iMod), 24. mai 2017

Protokoll fra foretaksmøte i Sykehuspartner HF, 31. mai 2017