DET KONGELIGE
HELSE- OG OMSORGSDEPARTEMENT

Direktoratet for e-helse
Postboks 6737 St. Olavs plass
0130 OSLO

Deres ref	Vår ref	Dato
	17/1131	09.06.2017

Tillegg til tildelingsbrev nr 4. - informasjonssikkerhet ved bruk av private leverandører

Direktoratet for e-helse gis i oppdrag å gjennomgå informasjonssikkerhet ved bruk av private underleverandører i helse- og omsorgssektoren.

Helsetjenesten 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. Disse leverandørene har en sentral rolle i å tilpasse og innføre nye løsninger i helse- og omsorgstjenesten, gjennomføre nødvendig service og vedlikehold, og til en viss grad også bistå i drift og forvaltning. Helse- og omsorgstjenesten må gi og styre tilganger til personell fra leverandørene for å kunne få utført nødvendige oppgaver.

Bakgrunn

Helse- og omsorgsdepartementet mottok 24. mai i år en foreløpig redegjørelse utarbeidet av PwC etter en gjennomgang av Sykehuspartner HF og Helse Sør-Øst RHFs håndtering av den planlagte tjenesteutsettingen knyttet til drift og modernisering av IKT-infrastruktur til Enterprise Services Norge AS (ESN).

Redegjørelsen fra PwC viser at det har vært en svikt i Sykehuspartner HFs gjennomføring av prosjektet. Sykehuspartner har ikke hatt en sentral oversikt over hvilke tilganger som har blitt gitt, og beslutninger om tilganger har etter PwCs 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

Postadresse	Kontoradresse	Telefon*	Avdeling	Saksbehandler
Postboks 8011 Dep	Teatergt. 9	22 24 90 90	E-helseavdelingen	Ilyass Koubaa
0030 Oslo		Org no.		22 24 86 80
postmottak@hod.dep.no	www.hod.dep.no	983 887 406		

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. For en fullstendig oversikt over PwCs vurderinger vil vi vise til vedlagte redegjørelse datert 24. mai d.å. Rapporten følger vedlagt.

Oppdrag

Direktoratet for e-helse gis i oppdrag å identifisere og foreslå gode rutiner for å sikre at de til enhver tid gjeldende krav til informasjonssikkerhet ved bruk av private leverandører etterleves.

Direktoratet skal som del av oppdraget utarbeide en overordnet status for bruk av nasjonale og internasjonale leverandører av tjenester som kontinuerlig eller episodisk arbeider inn mot virksomhetens datasystemer og under hvilke betingelser dette skjer.

Det skal videre utarbeides et sett med kriterier eller betingelser som bidrar til at denne formen for tjenester skjer på en ansvarlig måte og i tråd med de til enhver gjeldende krav.

Det er i denne sammenheng også relevant å vurdere om det er tjenester som ikke bør overlates til private underleverandører. Spesielt har departementet sett behov for at det sees på hvilke situasjoner og hvordan det eventuelt bør og kan skilles mellom norske, EØS-baserte og globale underleverandører, herunder behovet for å se på forholdet mellom helsetjenesten og sikkerhetsloven.

Som juridisk ramme for arbeidet vises det blant annet til helseforetaksloven §28, pasientjournalloven §22 og 23, personopplysningsforskriften kapittel 2, og forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten.

For å sikre et godt grunnlag skal Direktoratet for e-helse i sitt arbeid med oppdraget:

- Invitere representanter fra spesialisthelsetjenesten, andre relevante helsetjenesteaktører og helseforvaltningsorganer som behandler pasientinformasjon til å delta i arbeidet.
- Invitere følgende aktørgrupper til å gi innspill:
    - andre sentrale kompetansemiljøer, herunder Nasjonal sikkerhetsmyndighet
    - fagorganisasjoner, tillitsvalgte og brukerorganisasjoner
    - representanter for IKT-næringen

Frist for tilbakemelding

Helse- og omsorgsdepartementet ber om å få oversendt rapporten innen 1. november 2017.

Direktoratet for e-helse skal oversende en plan for gjennomføring av oppdraget innen tirsdag 27. juni.

Med hilsen

Bjørn Astad (e.f.)
ekspedisjonssjef

Ilyass Koubaa
konsulent

Dokumentet er elektronisk signert og har derfor ikke håndskrevne signaturer