Riksrevisjonen

Vår saksbehandler
Beate Seim Midtlien 22241255
Vår dato 12.11.2014
Vår referanse 2014/01468-3
Deres dato
Deres referanse

HELSE- OG OMSORGSDEPARTEMENTET
Postboks 8011 Dep
0030 OSLO

Høring - Forskrift om tilgang til helseopplysninger mellom virksomheter

Det vises til brev av 19. september 2014 fra Helse- og omsorgsdepartementet vedlagt høringsnotat om tilgang til helseopplysninger mellom virksomheter. Fristen for å avgi høringsuttalelse er 14. november 2014.

Riksrevisjonen har i forbindelse med selskapskontrollen for 2013 gjennomført en undersøkelse der målet har vært å vurdere om helseforetakenes styring og kontroll av tilgang til helseopplysninger i EPJ-systemet er i samsvar med gjeldende regelverk der tilgang kun kan gis for ansatte innen samme virksomhet.

Undersøkelsen, som omfattet Oslo universitetssykehus HF, Helse Bergen HF, St. Olavs Hospital HF og Universitetssykehuset Nord-Norge HF, ble rapportert til Stortinget 11. november 2014 i Dokument 3:2 (2014–2015). Dokumentet er tilgjengelig på https://www.riksrevisjonen.no/rapporter/Sider/Selskapskontrollen2013.aspx

Til Stortinget er Riksrevisjonens merknader til undersøkelsen oppsummert slik:

- Helseforetakene har ikke i tilstrekkelig grad implementert gjeldende regelverk om informasjonssikkerhet og behandling av helseopplysninger.
- Ansatte i helseforetakene har tilgang til helseopplysninger utover tjenstlig behov.
- Helseforetakene har ingen systematisk kontroll og oppfølging av ansattes tilganger til EPJ.
- Helseforetakene har mangelfull internkontroll av tilgangsstyringen i EPJ.

Ikrafttredelse og påfølgende implementering av ny pasientjournallov og forskrift, som gir elektronisk tilgang til helseopplysninger mellom virksomheter, vil etter Riksrevisjonens syn fordre at helseforetakene har et langt bedre kontrollregime på tilgangsstyringen i EPJ-systemet enn resultatet av ovennevnte undersøkelse viser.

Ifølge høringsnotatet skal en virksomhet som gir annen virksomhet tilgang, påse at denne virksomheten ivaretar kravene til informasjonssikkerhet ved behandling av opplysninger etter forskriften. Etter Riksrevisjonens vurdering er ikke administrerende direktør i de fire undersøkte helseforetakene per i dag i stand til å overholde sin plikt som databehandlingsansvarlig. Uten vesentlige forbedringer av eget kontrollregime vil det etter Riksrevisjonens syn derfor være svært vanskelig å påse at kravene til informasjonssikkerhet ved behandling av opplysninger er oppfylt i annen virksomhet.

Virksomhetene blir i forslaget til forskrift pålagt å etablere nødvendige organisatoriske og tekniske tiltak for tildeling og kontroll av tilgangsrettigheter til helseopplysninger. Riksrevisjonens undersøkelse viser at helseforetakene har mangelfulle rutiner for vurdering og kontroll av individuelt tjenstlig behov, og at det er svakheter i implementeringen av EPJ-systemene. Etter Riksrevisjonens syn bør det ryddes opp i disse forholdene, før det gis tilgang til helseopplysninger mellom virksomheter.

Ifølge forslaget skal den databehandlingsansvarlige løpende kontrollere hvem som har benyttet tilgangen og hentet frem helseopplysninger. Riksrevisjonens undersøkelse viser at ingen av helseforetakene gjennomfører systematiske loggkontroller på eget initiativ for å avdekke ureglementerte oppslag, noe som gjør at det nærmest vil være tilfeldig om snoking i pasientjournalene blir oppdaget. Før ny forskrift blir implementert bør det etter Riksrevisjonens menig bli utviklet verktøy og iverksatt tiltak som er egnet for å oppdage urettmessig tilegnelse av helseopplysninger.

Forskriften skal ifølge høringsnotatet bidra til at pasienter og brukere skal kunne ha tillit til at opplysningen i systemene blir sikret på best mulig måte og ikke tilflyter uvedkommende. Riksrevisjonens undersøkelse viser at tilgangsstyringen innad i fire av landets største helseforetak er mangelfull, og at helseforetakene på det nærværende tidspunkt sannsynligvis ikke er modne for å ivareta kravene til informasjonssikkerhet ved elektronisk deling av helseopplysninger mellom virksomheter. Uten en vesentlig forbedring av de forholdene Riksrevisjonen har påpekt, vil tilgang til helseopplysninger mellom virksomheter kunne medføre økt risiko for at sensitive og strengt taushetsbelagte personopplysninger tilflyter uvedkommende.

Etter fullmakt

Therese Johnsen
ekspedisjonssjef

Hege Merethe Herland
avdelingsdirektør