DET KONGELIGE FORNYINGS-,
ADMINISTRASJONS- OG KIRKEDEPARTEMENT

Helse- og omsorgsdepartementet
Postboks 8011 Dep
0030 OSLO

Unntatt offentlighet iht.
offentlighetsloven § 14
første ledd

Deres referanse	Vår referanse	Dato
201001921-/ASD	201001914-/AKH	13.09.2010

Høring av forslag til forskrift om informasjonssikkerhet, tilgangsstyring og tilgang til helseopplysninger i behandlingsrettede helseregistre

Vi viser til Helse- og omsorgsdepartementets brev av 03.06.2010 om ovennevnte.

Vi viser til Helse- og omsorgsdepartementets (HOD) brev av 10. mai 2010 med høringsnotat vedrørende utkast til forskrift om informasjonssikkerhet ved tilgangsstyring og tilgang til helseopplysninger i behandlingsrettede helseregistre.

Den økende elektroniske behandlingen av helseopplysninger gir muligheter, men skaper også utfordringer for informasjonssikkerheten hos virksomhetene. Elektronisk behandling bidrar til at pasientopplysningene enklere og raskere kan gjøres tilgjengelig både internt i en virksomhet og eksternt utenfor virksomheten. Fornyings-, administrasjons- og kirke-departementet (FAD) mener dette er en stor fordel med hensyn til bedre pasient-behandling og økt effektivisering av sektoren, forutsatt at helseopplysningene kun gjøres tilgjengelig for rett vedkommende til rett tid.

FAD oppfatter at høringsnotatet fra HOD er grundig bearbeidet. Foreliggende forskriftsutkast er et viktig steg i riktig retning for å oppnå balanse mellom helsepersonellets behov for rask tilgang til nødvendige og relevante helseopplysninger i behandlingsøyemed og ivaretakelsen av pasientenes personvern.

I et personvernperspektiv anser FAD det som positivt at forskriftsbestemmelsene begrenser både hvilke formål og hvilke tjenesteytere de behandlingsrettede

Postadresse	Kontoradresse	Telefon	Administrasjonsavdelingen	Saksbehandler
Postboks 8004 Dep	Akersg. 59	22 24 90 90	Telefaks	Anne Kristine Hage
N-0030 OSLO		Org no.	22 24 27 14	22 24 48 51
		972 417 785		

helseregistrene skal kunne betjene. En god etterlevelse og oppfølging av skrankene for bruk kombinert med skjerpete krav til sikkerhet vil kunne ivareta personvernhensynene på en god måte. Ikke minst vil reglene om obligatorisk opplæring være viktig for å oppnå en praksis som er i samsvar med regelverket.

FAD deler HODs vurdering av viktigheten av å ivareta tillitsforholdet mellom behandlende helsepersonell og pasientene. I et personvernperspektiv er dette hensynet avgjørende for en god, ballansert avveining mellom effektiv pasientbehandling og ivaretakelse av pasientens interesse i at fortrolige og sensitive opplysninger beskyttes mot uberettiget innsyn.

Forskriftens kapittel I Innledende bestemmelser

Til § 1, Forskriftens formål

FAD vil anbefale at merknadene til formålsbestemmelsen tar inn ivaretakelse av tillitsforholdet mellom pasient og helsetjeneste slik dette er formulert i departementets vurderinger og forslag i pkt 4.1.3 i høringsnotatet. Likeledes at merknadene redigeres i samsvar med høringsnotatets 4.1.3, vedrørende betydningen av at formålet med forskriften er å styrke informasjonssikkerheten. Merknadene bør gjøre rede for at skjerpet sikkerhet er bakgrunnen for valget av ordlyden "god informasjonssikkerhet" framfor, "tilfredsstillende informasjonssikkerhet" i helseregisterloven § 16.

Til forskriftens tekst i § 1

Selve teksten i bestemmelsen bør endres i samsvar med det som uttales i pkt 4.2.3 vedrørende virkeområdet, der det fremgår tydelig at forskriften gjelder "når formålet er å yte helsehjelp til pasient". Vi foreslår derfor at ordlyden "tilbys" i § 1 bør erstattes med "ytes". Dette synes også å samsvare med ordlyden tidligere i samme setning "å gi helsepersonell nødvendig tilgang til helseopplysninger". Tilbud av helsehjelp må anses å ligge forut for en behandlingssituasjon og er i større grad betinget av overordnet administrasjon så som planlegging, resurser og oversikt over ventelister etc. Slike administrative oppgaver kan neppe være betinget av tilgang til personidentifiserbare helseopplysninger og synes heller ikke å være i samsvar med definisjonen "behandlingsrettet helseregister".

Til § 2, Forskriftens virkeområde

Vi oppfatter at HODs avklaring og innsnevring av virkeområdet er hensiktsmessig i et personvern- og sikkerhetsperspektiv, jf. også ovennevnte kommentarer.

Til § 3, Definisjoner

Vi anbefaler at forskriften enten bør henvise til definisjon av behandlingsrettet helseregister i helseregisterloven § 2 nr. 7, eller ta inn definisjonen i forskriften ettersom dette er et av de sentrale reguleringstemaene. Videre vil vi anbefale at de enhetene/områdene som skal omfattes av henholdsvis intern eller ekstern virksomhet defineres på en tydelig måte. Det er vesentlig å sørge for en entydig forståelse av hvilke områder som omfattes av hvilken type tilgangsregulering, ikke minst av hensyn til pasientens ubetingete rett til å samtykke dersom informasjon skal overføres til en annen virksomhet. Ettersom det skjer omfattende fusjoner av store virksomheter innenfor helsetjenestene, kan det vurderes om det er mer

hensiktsmessig å regulere "enheter" eller "behandlingsområder" enn virksomheter, når intensjonen er å begrense kretsen av tilgangsberettigete. Hvis det for eksempel er slik at alle helseforetak under ett regionalt helseforetak er å anse som internt, har sondringen mellom ekstern og intern tilgang liten reell betydning.

Kapittel II Generelle krav til informasjonssikkerhet

Selve tittelen på forskriften tilsier at sikkerhetsreguleringen er spesielt knyttet til behandlingsrettede helseregistre, jf. også de uttalelser som gis om formål og de skjerpede krav til sikkerhet i punkt 4.3.1 i høringsnotatet. Det kan derfor virke uklart hvorfor det gis generelle regler i denne sammenhengen; de generelle reglene finnes i helseregisterloven, personopplysningsloven og personopplysningsforskriften. I tillegg er det også utarbeidet omfattende krav til sikkerhet i "norm for informasjonssikkerhet i helsesektoren". Ettersom de generelle reglene ikke gjengis i sin helhet, vil det derfor være behov for å vurdere det øvrige regelverket vedrørende krav til sikkerhet i tillegg til forskriftens krav. Dette kan tale for at denne forskriftens sikkerhetsregulering bør ha som mål å synliggjøre de skjerpete kravene til informasjonssikkerhet i samsvar med formålet med forskriften. Instruks eller fotnoter kan brukes for å henvise til de samlete kravene til sikkerhet i slike systemer.

De generelle kravene sier lite utover virksomhetenes ansvar for å etablere strategi, planverk og rutiner uten nærmere innhold. I så måte ligner de generelle bestemmelsene mer om en instruks enn en forskrift. I den grad sikkerhetsbestemmelsene også må antas å være av betydning for pasientenes krav på vern om sine opplysninger, gir disse bestemmelsene ingen holdepunkter for en pasient til å vurdere om forskriften overholdes eller ikke, før ev. pasienten ber om en etterfølgende kontroll ved innsyn i logg. Videre kan det vel stilles spørsmål ved om bestemmelser av et slikt innhold kan kvalifisere for straffesanksjonering jf. forskriftens §§ 35 og 36. Vi foreslår at de generelle reglene kan vedlegges som instruks til virksomhetens ledelse og den databehandlingsansvarlige.

Sikkerhetsspørsmål må være gjenstand for interesse og ansvar på alle nivåer i sektoren. Innarbeiding av en sikkerhetskultur i sektoren vil kreve både lederskap og omfattende deltakelse hos den enkelte. Det bør fremgå tydelig at det er et lederansvar å sørge for at dette skjer, jf. forslag til forskrift § 7 Sikkerhetsledelse.

Kapittel V Tilleggsbestemmelser for direkte tilgang til helseopplysninger i behandlingsrettet helseregister på tvers av virksomheter

Det kan spørres om betydningen av § 24, annet ledd, vedrørende sikkerhetsvurderinger ved ekstern overføring av sensitive opplysninger til annen virksomhet. Som et utgangspunkt vil enhver økning av tilgangsberettigete til et informasjonssystem øke risikoen for lekkasje av informasjon. Ved å utvide kretsen av tilgangsberettigete til også å omfatte ansatte fra andre virksomheter inn i eget system, kan det synes som umulig å garantere for at sikkerheten ikke svekkes.

For øvrig er FAD positiv til den klare bestemmelsen i § 27 som gir pasienten avgjørende myndighet til å beslutte om helseopplysningene kan deles med andre virksomheter. Vi mener også at det er viktig at unntaksregelen er gjort snever. I tillegg er det viktig at

pasientens rett til å sperre opplysninger ivaretas samt rett til innsyn i logg. Det bør også være et vilkår for å kunne inngå avtaler på tvers av virksomheter at loggsystemet oppfyller visse minimumskrav for systematiske etterkontroller.

Administrative og økonomiske konsekvenser

Av høringsutkastet fremgår det at god informasjonssikkerhet i sektoren vil kreve organisatoriske så vel som tekniske og fysiske tiltak. I denne sammenheng er det også viktig at sikkerhetsarbeidet blir satt i system slik at dette kan blir fulgt opp på en forsvarlig måte. HOD må følgelig sørge for at virksomhetene blir pålagt å avsette tilstrekkelig med interne ressurser til å kunne følge opp sikkerhetsarbeidet i den enkelte virksomhet.

Med hilsen

Marianne Hauan Molstad (e.f.)
avdelingsdirektør

Anne Kristine Hage
rådgiver