

Vår dato	Vår referanse
13.11.2014	14/00921-2
Deres dato	Deres referanse
	14/3724

Helse- og omsorgsdepartementet
Postboks 8011 Dep
0030 Oslo

Saksbehandler:
Britt Eva Bjerkvik Haaland

postmottak@hod.dep.no

Hørings svar - Forslag til forskrift om tilgang til helseopplysninger mellom virksomheter

Vi viser til høringsbrev av 19. september.2014 der Helse- og omsorgsdepartementet sender forslag til forskrift om tilgang til helseopplysninger mellom virksomheter på høring.

Generelle bemerkninger

Departementet sier i høringsnotatet at det ikke vil være hensiktsmessig med konkrete tekniske krav i forskriften. Difi stiller seg positive til detaljeringsnivået i forskriften. Det er alltid en fare for at en forskrift som denne blir så detaljert og teknisk at den etter kort tid ender opp med å stille krav som ikke er på høyde med den beste teknologien på området. En detaljert forskrift vil derfor kunne være til hinder for at virksomhetene tar i bruk ny og bedre teknologi. Ved å stille krav til hva som skal oppnås, slik forskriften nå gjør, har databehandlingsansvarlig mulighet til å sette i verk de tiltak som til enhver tid gir den mest hensiktsmessige løsning basert på de risikovurderinger som foretas. Dette legger til rette for utvikling og for at behovene og rettighetene til pasienter og brukere ivaretas på en best mulig måte.

Difi synes det er positivt at det settes fokus på at informasjonssikkerhet (og personvern) er mer enn konfidensialitet og at det også legges vekt på viktigheten av tilgjengelighet og integritet.

Vi forstår det slik at tilgangsstyringen i helse- og omsorgssektoren gir utfordringer. Hvor mange som reelt sett har adgang til å se pasientopplysninger, vil i dag variere ut fra virksomhetens størrelse og hvordan tilgangsstyring er tatt i bruk. De samme utfordringene ved tilgangsstyring og hendelsesregistrering (logging) som oppstår ved tilgang til pasientopplysninger internt i en virksomhet, vil også oppstå ved tilgang på tvers av virksomhetsgrenser. Viktige tiltak som må være på plass for å ivareta informasjonssikkerheten, uavhengig av virksomhetsgrenser, er bl.a. gode tilgangsregimer, tilfredsstillende logging, adgang til enkel innsyn i logg for pasienten og retten til å motsette seg kommunikasjon av opplysninger (sperring). Det er viktig at virksomhetene har fokus på dette både i sitt arbeid med informasjonssikkerhet internt i virksomheten, og ved tilgang til journalsystemer på tvers av virksomhetsgrenser.

Forskriftens formål

Difi stiller seg positive til at det legges bedre til rette for sikker tilgang til helseopplysninger mellom virksomheter for å yte, administrere og kvalitetssikre helsehjelp til den enkelte.

Det er viktig at slik tilgang skal sikre bedre helsehjelp til den enkelte i tillegg til å effektivisere eksisterende informasjonsdeling. Tilgang vil kunne gi helsemessige gevinster, for eksempel ved at behandlingsforløp kan gjennomføres raskere eller ved å unngå at undersøkelser blir gjentatt. For eksempel peker Statens strålevern i høringsuttalelsen til pasientjournalloven på at uhensiktsmessige radiologiske undersøkelser er en økende utfordring ettersom det er til pasientens beste å ikke utsettes for mer stråling enn nødvendig.

Det er positivt at departementet fastslår at tilgang mellom virksomheter forutsetter risiko-vurderinger, rutiner og tilfredsstillende tekniske og organisatoriske løsninger. Utgangspunktet for vurderingen bør være at tilgang på tvers av virksomhetsgrenser i stor grad gir de samme informasjonssikkerhetsmessige utfordringer som arbeid internt.

Det er bra at det påpekes at forskriften ikke pålegger noen virksomheter plikt til å gi tilgang og at virksomheter som ikke har tilstrekkelig strukturerte journaler, ikke kan åpne for tilgang for andre virksomheter. Det er altså ikke et frislipp av helseopplysninger, kun en mulighet for de virksomheter som har de tekniske og organisatoriske forutsetningene som kreves.

Helsevesenet i Norge i dag består av virksomheter som er svært ulike i type, størrelse, organisering og teknologisk modenhet. Forskriften gjør det mulig for de virksomhetene som har kapasitet til å ta i bruk mulighetene, å gjøre dette uten å bli bremsert av de virksomhetene som ikke er klare. Også innenfor den enkelte virksomhet, er det forskjeller på hvilke opplysninger det kan være relevant å gi til helsepersonell i andre virksomheter. At det kan skilles mellom ulike typer helseopplysninger, ulike typer helsepersonell/roller og ulike situasjoner, er positivt. Helsevesenet i Norge består av et stort spenn av virksomheter. Fra de små fastlege- eller fysioterapeutpraksisene med bare en eller et fåtall ansatte og en begrenset mengde helseopplysninger, til de store helseforetakene med mange tusen ansatte og et vell av helseopplysninger, både i antall og type. Med den nye forskriften, blir det mulig å lage løsninger som er tilpasset ulike organisasjonsformer og organisasjonsstørrelser. Dette stiller krav til virksomhetenes modenhetsnivå når det gjelder personvern og informasjonssikkerhet.

Forskriftens virkeområde – grensen mellom tilgang og utlevering

Forskriften skal kun gjelde tilgang og ikke utlevering. Vi opplever imidlertid at grensen mellom disse to er noe uklart beskrevet. I punkt 5.6.2 i høringsnotatet heter det at helseopplysninger som hentes fram ved hjelp av automatiske spørre-svar funksjoner, skal anses som utlevering og derfor ikke dekkes av forskriften. Dette kan forstås som at en automatisert innhenting av journalopplysninger (forutsatt at systemet kontrollerer at samtykke foreligger), skal kunne gjøres uten at forskriften kommer til anvendelse. Er det tilsiktet? Uten en nærmere beskrivelse av hvor grensen skal trekkes mellom tilgang og utlevering, vil det være fare for at virksomheter definerer seg bort fra forskriften. Man risikerer da at det gis bredere adgang til pasientopplysninger uten at kravene til informasjonssikkerhet i forskriften trenger å ivaretas. Difi ønsker derfor en ytterligere presisering av hva som ligger i tilgang til opplysninger, slik at det kommer tydelig frem når forskriften kommer til anvendelse.

Avtale

I forslag til § 3 og § 4, gjøres det klart at de databehandlingsansvarlige virksomhetene må ha inngått avtale om tilgang mellom virksomheter. Det er bra at databehandlingsansvarlig må gjøre konkrete behovs- og risikovurderinger for at slik avtale kan inngås. Det fremgår ikke av høringsnotatet om en slik avtale kan inngå som en del av et eksisterende avtaleregime mellom virksomhetene. Om vilkårene i § 4 er oppfylt, må det også være mulig å la avtalen inngå som en del av andre avtaler mellom virksomhetene for å forenkle avtaleregimet mellom dem.

Informasjon til pasienten

I § 8, 3. ledd, er det uklart hva virksomheter som henter frem opplysninger plikter å informere pasientene om. Vi foreslår derfor følgende endringer i tredje ledd

Den databehandlingsansvarlige i virksomheter som henter frem opplysninger etter denne forskriften skal informere pasienten blant annet om

- a) hvilken virksomhet opplysningene er hentet fra,*
- b) hvilke opplysninger tilgangen omfatter, og*
- c) at pasienten kan motsette seg at det gis tilgang, jf. § 9.*

Dokumentasjon av tilgang.

Ved tilgang på tvers av virksomhetsgrenser er det viktig at virksomhetene har en klar ansvarsfordeling, blant annet ved ivaretagelse av logging og oppfølgingen av denne. Uavhengig av hvilke tekniske løsninger som tas i bruk, er det viktig å fokusere på tydelige roller og ansvar for å sørge for tilfredsstillende sikkerhet og ivaretagelse av pasientens rettigheter.

Vi ser det som positivt at tilgang skal dokumenteres automatisk. Det er noe uklart om dokumentasjonskravene i §10 gjelder bare for avgivende virksomhet eller om de gjelder for begge. Dersom det er ment at de skal gjelde begge virksomheter har, foreslår vi følgende tilføyelse i § 10:

«...skal dokumenteres automatisk i både avgivende og mottakende virksomhet.»

Dersom det er slik å forstå at § 10 kun skal gjelde for avgivende virksomhet og § 11 kun for mottakende virksomhet, bør det komme klart fram at virksomhetene skal ha mulighet for innsyn i hverandres logger. Det bør også komme frem hvorvidt pasient/bruker kan be om innsyn i logger fra begge virksomheter ved å henvende seg til kun en av dem.

Vennlig hilsen
for Difi

Lillian Røstad
seksjonssjef

Britt Eva Haaland
seniorrådgiver

Dokumentet er godkjent elektronisk og har derfor ingen håndskrevne signaturer.