Direktoratet for forvaltning og IKT

Vår dato	Vår referanse
15.10.2013	13/00959-2
Deres dato:	Deres referanse
	13/2992

Helse- og omsorgsdepartementet
Postboks 8011 Dep
0030 Oslo

Saksbehandler:
Caroline Ringstad Schultz

Høringssvar - Forslag til ny pasientjournallov og ny helseregisterlov

Vi viser til brev av 28.06.2013 der Helse- og omsorgsdepartementet sender på høring forslag til ny pasientjournallov og helseregisterlov.

1. Generelle bemerkninger

Dagens helseregisterlov trådte i kraft 01.01.2002. Siden den gang har både teknologien og organiseringen i helse- og omsorgssektoren endret seg, noe som også har ført til endret behov og teknologiske muligheter for kommunikasjon av pasientopplysninger. Difi stiller seg derfor positive til at dagens helseregisterlov foreslås endret, bl.a. for å åpne opp for bruk av nye kommunikasjonsformer og metoder.

Elektronisk samhandling skjer på tvers av sektorer, og det er derfor viktig med felles forståelse av begreper og krav på tvers av sektorer så langt dette er hensiktsmessig. Difi er derfor positive til at begrepet «informasjonssikkerhet» nå foreslås å ha likelydende ordlyd i helseregisterloven, pasientjournalloven og personopplysningsloven ved at ordet «kvalitet» er foreslått fjernet fra lovforslagets forslag til bestemmelser om informasjonssikkerhet.[1]

2. Informasjonssikkerhet

2.1. Kravstillelse og ansvar

Difi mener prinsipielt, som lovutkastet legger opp til, at det er den databehandlingsansvarlige som bør fastsette konkrete krav til informasjonssikkerhet innenfor lovverkets angitte rammer basert på en vurdering av risiko. Krav til informasjonssikkerhet kan f.eks. endre seg over tid utfra den teknologiske utviklingen, endret risikobilde m.m., og det er derfor positivt at dette

[1] Utkast til pasientjournallov § 22 og helseregisterlov § 18.

Direktoratet for forvaltning av IKT (Difi)
Postboks 8115 Dep, 0032 Oslo
Telefon: 22 45 10 00

Besøksadresse Oslo:
Grev Wedels plass 9
Telefaks Oslo: 22 45 10 01

Besøksadresse Leikanger:
Skrivarvegen 2
Telefaks Leikanger: 57 65 50 55

postmottak@difi.no
Org.nr.: NO 991 825 827
www.difi.no

gjenspeiles i lovforslaget. En slik risikobasert tilnærming gir fleksibilitet, men stiller samtidig høye krav til kompetansen i den enkelte virksomhet. Det er dermed et behov for veiledningsmateriale som omtaler hvordan risiko kan reduseres og tilstrekkelig sikkerhetsnivå etableres, eksempelvis slik det er gjort i forbindelse med Norm for informasjonssikkerhet for helse- og omsorgssektoren.

Difi stiller seg også positive til at det legges bedre til rette for tilgang på tvers av virksomhetsgrenser ved at forbudet i nåværende helseregisterlov § 13 oppheves. Ved å endre bestemmelsen vil virksomhetene ha mulighet til å foreta gode avveininger av hensynene til konfidensialitet og tilgjengelighet, og på denne bakgrunn kunne etablere fellesløsninger eller gi ansatte i andre virksomheter adgang til å benytte egne, etablerte løsninger. Det blir den databehandlingsansvarlige som er ansvarlig for å beslutte hvordan opplysningene tilgjengeliggjøres, og sørge for at sikkerheten ivaretas.

2.2. Utfordringer

Difi støtter endringen i helseregisterloven § 13, men ønsker å synliggjøre visse utfordringer som det må jobbes videre med. Dette gjelder både utfordringer som kan løses lokalt i den enkelte virksomhet, men også på et myndighetsnivå f.eks. i form av veiledning og publisering av veiledningsmateriell.

Det er spesielt tre forhold Difi ønsker å trekke frem:

- Tilgangsstyring
  Difi forstår det slik at det tidligere har vært utfordringer med manglende styring og kontroll med tilgangen til pasientopplysninger i helse- og omsorgssektoren.[2] I dag vil antallet som reelt sett har adgang til å se pasientopplysninger varierer utfra virksomhetens størrelse og hvordan tilgangsstyring er implementert. Mange av de samme utfordringene til tilgangsstyring som oppstår ved tilgang til pasientopplysninger internt i en virksomhet vil også oppstå ved tilgang på tvers av virksomhetsgrenser.

  Ved tilgang på tvers blir det spesielt sentralt å fokusere på gode prosesser for autorisering og autentisering. Det blir f.eks. viktig å sørge for at ansatte kun autoriseres til å få adgang til relevante opplysninger i andre virksomheter, og at virksomhetene har mulighet til å kontrollere autorisasjoner gjort av andre virksomheter.

[2] Se bl.a. Datatilsynets rapport «sviktende tilgangsstyring i elektroniske pasientjournaler?» (2009), http://www.datatilsynet.no/verktoy-skjema/Publikasjoner/Analyser-utredninger/Sviktende-tilgangsstyring-i-elektroniske-pasientjournaler1/

- Oppfølgning og kontroll
  Det blir viktig å ha gode kontrollmekanismer for å avdekke uheldige hendelser og urettmessig tilgang til pasientopplysninger. Ved tilgang på tvers av virksomhetsgrenser må det sørges for at virksomhetene følger opp egne hendelser, kontrollerer bruken av systemene, og at det foreligger en klar ansvarsdeling mellom involverte virksomheter for oppfølgning av hendelser som involverer flere virksomheter.

- Ansvarsdeling mellom involverte virksomheter
  Ved tilgang på tvers av virksomhetsgrenser er det viktig at virksomhetene har en klar ansvarsdeling. Dette gjelder bl.a. oppfølgning og kontroll av tilgangsstyringen og pasientens rett til informasjon og innsyn i egne opplysninger. Uavhengig av de tekniske løsningene som tas i bruk, blir det derfor viktig å fokusere på tydelige roller og ansvar mellom de involverte virksomhetene for å sørge for tilfredsstillende sikkerhet og ivaretakelse av pasientens rettigheter.

3. Foreslått regulering av informasjonssikkerhet og internkontroll

Forslaget til helseregisterlov og pasientjournallov viderefører tidligere bestemmelser om informasjonssikkerhet og internkontroll i henholdsvis forslag til ny helseregisterlov §§ 18 og 19 og pasientjournallov §§ 22 og 23. Bestemmelsene samsvarer i stor grad med tilsvarende bestemmelser i personopplysningsloven §§ 13 og 14.

Difi publiserte i desember 2012 en rapport om styringssystem for informasjonssikkerhet.[3] Rapporten gjengir en del erfaringer fra forvaltningen. Erfaringer som fremheves er bl.a.:

- volumet av dokumentasjon bør bestemmes utfra en vurdering av risiko, vesentlighet og virksomhetens egenart
- der styringssystem for informasjonssikkerhet inngår som en del av virksomhetens helhetlige styrings- og kvalitetssystem, når man bedre ut i hele organisasjonen med relevante risikovurderinger og bevissthet om informasjonssikkerhet

Dette er viktige funn som er fulgt opp i senere arbeid. Fornyings-, administrasjons- og kirkedepartementets har bl.a. foreslått endringer i e-forvaltningsforskriftens § 13 om informasjonssikkerhet. Disse endringene skal bidra til å presisere at styringssystemet/internkontrollen og omfanget av denne må tilpasses risikoen, og at styringssystemet/internkontrollen innen informasjonssikkerhet med fordel kan være en del av det helhetlige styringssystemet/internkontrollen i virksomheten.[4]

---

[3] Styringssystem for informasjonssikkerhet - erfaringer med og anbefalinger om standardene ISO 27001 og ISO 27002, rapport 2012:15.
http://www.difi.no/filearchive/difi-rapport-2012-15-styringssystem-for-informasjonssikkerhet.-erfaringer-og-anbefalinger.pdf

[4] Se digitaliseringsrundskrivets kapittel 1.7,
http://www.regjeringen.no/nb/dep/fad/dok/rundskriv/2013/digitaliseringsrundskrivet.html?id=734925, og forslag til endringer i eForvaltningsforskriften - digital kommunikasjon som hovedregel, § 13, andre ledd,

De samme hensynene som ligger bak de overnevnte endringene for e-forvaltningsområdet gjør seg også gjeldene for helse- og omsorgssektoren på generelt grunnlag. På denne bakgrunn kunne forslaget til ny helseregisterlov §§ 18 og 19 og pasientjournalloven §§ 22 og 23 fokusert ytterligere på at dokumentasjonskravet må tilpasses det risikobaserte behovet i den enkelte virksomhet, samt satt §§ 22 og 23 i en enda tydeligere sammenheng. Dette kunne f.eks. vært gjort gjennom å slå sammen bestemmelsene (helseregisterlov §§ 18 og 19 og pasientjournalloven § 22 og 23) til en felles bestemmelse om internkontroll, der informasjonssikkerhet inngår som et viktig element. Samtidig kunne det vært presisert i bestemmelsen at dokumentasjonskravet gjelder for «nødvendig» dokumentasjon, slik at virksomheten må foreta en vurdering av behovet for dokumentasjon utfra risiko, nødvendigheten av dokumentasjon og virksomhetens egenart. Disse endringene vil føre til et mer enhetlig regelverk der krav til internkontroll sees i sammenheng på tvers av fagområde.

4. Indirekte personidentifiserbare helseopplysninger

Departementet foreslår å fjerne definisjonene av pseudonyme og avidentifiserte helseopplysninger jf. dagens helseregisterlov § 2 nr. 2 og 4. Begrepene foreslås erstattet av det bredere begrepet «indirekte personidentifiserbare helseopplysninger» jf. utkast til ny helseregisterlov § 1 nr. 2. Samtidig foreslås det at «indirekte personidentifiserbare helseopplysninger» ikke skal være omfattet av taushetsplikt i visse situasjoner, jf. utkast til ny helseregisterlov § 17. Bestemmelsen skal gjelde for registre som opprettes med forskrift med hjemmel i § 8, og der opplysningene skal benyttes til kvalitetssikring, forskning, planlegging og styring av helse- og omsorgstjenesten.

Difi vil peke på at «indirekte personidentifiserbare helseopplysninger» kan gjelde svært følsomme forhold. Regional etisk komité (REK), Helsedirektoratet og andre databehandlingsansvarlige for sentrale helseregistre har derfor i flere sammenhenger stilt strenge krav til håndtering av opplysninger hvor kombinasjoner av flere opplysninger kan føre til en identifisering av den registrerte. Difi savner en nærmere vurdering av konsekvensene av at taushetsplikten oppheves for denne typen opplysninger, herunder om det vil kunne svekke tillitsforholdet mellom pasient og behandler at opplysninger fra et behandlingsforløp rapporteres inn til et register og senere utleveres som indirekte identifiserbare. En slik vurdering bør sees i sammenheng med at adgangen til å opprette sentrale helseregistre foreslås overført fra Stortinget til Kongen i statsråd, jf. utkast til helseregisterlov § 8. Videre vil ulempen for den registrerte kunne variere utfra hvor mange opplysninger som ønskes utlevert, og i hvilken grad de beskriver særlig intime eler stigmatiserende forhold. Således vil konsekvensen ved utilsiktet utlevering kunne variere sterkt. Difi antar dette er forhold som bør utredes nærmere før et slikt lovhjemlet unntak fra taushetsplikten vedtas.

---

http://www.regjeringen.no/nb/dep/fad/dok/horinger/horingsdokumenter/2013/horing-digital-kommunikasjon.html?id=730027.

Vennlig hilsen
for Difi

Tone Bringedal
Avdelingsdirektør

Caroline Ringstad Schultz
Seniorrådgiver

Dokumentet er godkjent elektronisk og har derfor ingen håndskrevne signaturer.