NOTAT KITH

Forfatter *Torbjørn Nystadnes, KITH*

Dato *9. mars 2010* **KITH-notat nr. 1004**

Forslag til kombinert modell for helseregistre

Sammendrag

I dette notatet skisseres en løsning for helseregistre som kombinerer egenskapene ved et pseudonymt helseregister med muligheter for personidentifiserbare opplysninger for de pasienter som har samtykket til det. For å synliggjøre at en slik kombinert modell både vil kunne ivareta behovet for kvalitetssikring av avgitte opplysninger og behovet for å kunne kontakte enhver pasient, er det utarbeidet et sett av overordnede krav.

Avslutningsvis er det også tatt med noen betraktninger rundt kostnadene forbundet med en slik kombinert modell sett i relasjon til kostnadene forbundet med registre hvor identiteten lagres kryptert og hvor hvert enkelt register selv håndterer kryptering og dekryptering av identiteten. Konklusjonen her er at kostnadene ikke vil være vesensforskjellige.

Bakgrunn

Om fellesregistermodellen

I rapporten *Gode helseregistre - bedre helse*[1] foreslås det en framtidig modell for håndtering av helseregistre, "fellesregistermodellen".

Modellen innebærer etablering av et sett av basisregistre med personidentifiserbare opplysninger som skal samles inn uten samtykke fra den enkelte. I tillegg skal det i tilknytning til hvert basisregister etableres et sett av medisinske kvalitetsregistre med personidentifiserbare opplysninger hvor pasienter etter forslaget skal kunne reservere seg mot registrering.

Elleve mulige kandidater til slike fellesregistre er nevnt i rapporten:

1. Kreftsykdom
2. Fødsel, barn og unge (inkludert sjeldne tilstander, syndromer og misdannelser)
3. Hjerte- og karsykdom
4. Diabetes (type I og II)
5. Infeksjonssykdommer
6. Legemidler

[1] Gode helseregistre - bedre helse, Strategi for modernisering og samordning av sentrale helseregistre og medisinske kvalitetsregistre 2010–2020. Hovedrapport fra forprosjektet Nasjonalt helseregisterprosjekt. Folkehelseinstituttet 2009.

7. Psykiske lidelser (inkludert rusmisbruk)
8. Muskel- og skjelettsykdom (inkludert giktsykdom, brudd, proteser)
9. Nevrologiske sykdommer
10. Luftveissykdommer
11. Ulykker, vold, traumer og intensivbehandling

Begrunnelsen for at opplysningene må være personidentifiserbare er todelt. For det første hevdes det at kjennskap til pasientens identitet er nødvendig for å kunne foreta kvalitetssikring av de opplysningene som avgis. For det andre vil det være behov for å kunne kontakte pasienter i forbindelse med konkrete forskningsprosjekt.

Kvalitetssikring som medfører behov for kjennskap til pasientenes identitet vil formodelig innebære at de som skal foreta kvalitetssikringen har behov for opplysninger fra pasientenes journaler. Dersom slik kvalitetssikring skal foretas av personale ved registret, må disse enten kunne gis direkte tilgang til enhver pasientjournal som har dannet grunnlag for rapportering til registeret, eller så må registret få ulevert kopier av pasientjournalene. Dersom alle de foreslåtte fellesregistre blir etablert, vil dette trolig innebærer at de fleste pasientjournaler i spesialisthelsetjenesten må være tilgjengelig for utvalgt personale ved registrene.

Selv om den modell som foreslås nok kan være utmerket sett fra et forskersynspunkt, er det ingen god modell sett fra et personvernsynspunkt. Det vil trolig være i fellesregistrene at hovedtyngden av de mest følsomme opplysningene vil finnes og dersom forslaget i rapporten tas til følge vil pasienten fratas enhver form for rett til medbestemmelse over disse opplysningene. En bør derfor søke å finne fram til en modell som kan ivareta personverninteressene på en bedre måte, og som samtidig legger forholdene til rette for god forskning.

Å realisere dette innenfor rammene av gjeldende lovgivning kan bli en utfordring.

Personentydige helseopplysninger

I helseregisterloven omtales to former for personentydige helseopplysninger:

1. Personidentifiserbare helseopplysninger
2. Pseudonyme helseopplysninger

Pseudonyme helseopplysninger innebærer at den registrertes identitet er kryptert og det stilles da ikke krav om samtykke fra den registrerte. Et sentralt krav er at ingen skal kunne ha tilgang til både pseudonym, identitet (f.eks. fødselsnummer) og helseopplysninger. Avgiver skal kun ha identitet og helseopplysninger, register kun pseudonym og helseopplysninger mens den tiltrodde pseudonymforvalteren (TPF) kun skal ha identitet og pseudonym.

For personidentifiserbare helseopplysninger omtaler loven tre alternativer:

a. Krav om samtykke fra den registrerte.
b. Uten samtykkekrav men med krav om at direkte personidentifiserende kjennetegn skal lagres kryptert.
c. Verken krav om samtykke eller krav til kryptering av identitet.

For registre som kan inneholde personidentifiserbare helseopplysninger med kryptert identitet, stilles det ikke spesifikke krav til hvordan kryptering av identitet skal gjennomføres. Det er heller ikke stilt konkrete krav til når dekryptering kan skje, men i forbindelse med

behandlingene av bestemmelsen om kryptert identitet, uttalte Stortingets helse- og omsorgskomiteens mindretall (representantene fra regjeringspartiene) at "kun et fåtall spesielt autoriserte medarbeidere kan utløse dekryptering".[2] Det samme mindretallet mente at "personidentifikasjonen [bør kunne] dekrypteres ved hjelp av en nøkkel som finnes internt i registeret". Ettersom mindretallets innstilling ble vedtatt, kan både kryptering og dekryptering skje internt i den virksomhet som er databehandlingsansvarlig eller databehandler for helseregistret.

Kombinert modell for registerhåndtering

Selv om det vel ikke er eksplisitt uttrykt i helseregisterloven, synes den allmenne oppfatning å være at alle opplysningene i et helseregister må være på samme form. Så langt er det i hvert fall ikke etablert noe helseregister som inneholder både pseudonyme helseopplysninger og personidentifiserbare helseopplysninger.

Men nettopp en slik kombinasjon vil trolig kunne løse en del av de problemene en står overfor her.

Et helseregister hvor helseopplysningene lagres med kryptert identitet dersom det foreligger samtykke fra den registrerte og på pseudonym form dersom slikt samtykke ikke foreligger, vil kunne bli komplett. Samtidig vil en for de som har gitt sitt samtykke, ha de samme muligheter som i den foreslåtte "fellesregistermodellen".

Ytterligere forbedringer både når det gjelder personvern og registerkvalitet bør kunne oppnås dersom det foretas en revidering av regelverket med sikte på å legge forholdene til rette for bruk av elektroniske løsninger som gir mulighet for elektronisk samhandling mellom avgiver og helseregister om bestemte pasienter, uten at pasientenes identitet trenger å være kjent for registeret. Tilsvarende bør en også legge til rette for at registret skal kunne kommunisere med den enkelte registrerte, fremdeles uten at registret har kjennskap til identiteten.

For å illustrere hvilke forhold som bør vurderes under revidering av regelverket, er det nedenfor tatt med noen krav som kan tenkes stilt til slike løsninger og bruken av dem.

1. De registrertes identitet (fødselsnummer og/eller andre typer personidentifikatorer) skal være kryptert. Krypteringen skal skje hos en tiltrodd pseudonymforvalter (TPF).
2. Kryptering av identitet skal skje på en slik måte at den krypterte identiteten fyller kravene til et pseudonym.
3. For de pasienter som har samtykket til det, skal identiteten kunne dekrypteres når dette er nødvendig for å oppnå formålet med registret.
4. All behandling av direkte personidentifiserbare opplysninger (dvs. opplysninger med dekryptert identitet), skal skje i et separat system, adskilt fra opplysninger med kryptert identitet.
5. For pasienter som ikke har samtykket til at identiteten kan dekrypteres, skal all behandling av de opplysninger som avgis, skje i henhold til gjeldende regler for håndtering av pseudonyme helseopplysninger.

---

[2] Innst. O. nr. 40 (2006-2007) om lov om endringer i helseregisterloven (Norsk pasientregister)

6. I den grad det er nødvendig for å oppfylle formålet med registret, skal det finnes en mulighet for å kontakte enhver pasient som ikke har reservert seg mot å bli kontaktet. Slik kontakt skal skje via TPF og den virksomhet som har avgitt de opplysningene som har dannet grunnlaget for ønsket om kontakt.
   Formålet med en slik kontakt kan f.eks. være å informere pasienten om et planlagt forskningsprosjekt og forespørre pasienten om å delta i det ved å samtykke til at prosjektet får tilgang til pasientjournalen.
7. Svar, herunder også avslag på forespørsel som nevnt foran, skal kunne sendes tilbake til den som har forespurt via TPF. Dersom en pasienter gir sitt samtykke til f.eks. å delta i et forskningsprosjekt, vil den videre kommunikasjon kunne skje direkte uten at TPF involveres.
8. I forbindelse med kvalitetssikring av opplysninger og i andre tilfeller som faller inn under registrets formål, skal det finnes en mulighet for å samhandle elektronisk med den virksomhet som har avgitt bestemte opplysninger til registret. Slik samhandling skal skje via TPF.
9. Dersom det avdekkes feil i opplysninger som er avgitt, skal dette meldes tilbake til den virksomhet som har avgitt opplysningene.
10. Så fremt det er nødvendig for å kvalitetssikre opplysninger som er avgitt fra en virksomhet, skal denne virksomheten kunne få utlevert opplysninger om den aktuelle pasienten som er avgitt fra andre virksomheter. Det skal ikke utleveres flere opplysninger enn det som er nødvendig for å kunne foreta kvalitetssikringen.

I rapporten *Gode helseregistre - bedre helse* gjøres det et stort poeng av at kvaliteten av de opplysninger som rapporteres til registrene er mangelfulle og at kjennskap til pasientens identitet er nødvendig for å kunne gjennomføre kvalitetssikring og foreta nødvendige korrigeringer av de avgitte opplysningene. Den kombinerte modellen som foreslås i dette notatet, innebærer at avgiver og register skal samarbeide om kvalitetssikringen og at de feil og mangler som avdekkes skal tilbakeføres til den enkelte pasients journal. Dette vil også være i tråd med det som på side 98 i rapporten *Gode helseregistre - bedre helse* angis som et langsiktig mål: "Mest mulig av kvalitetssikringen av data må skje der dataene registreres".

Sett fra et pasientperspektiv bør det være en klar fordel at eventuelle feil i journalen kan avdekkes og korrigeres. Feilaktige opplysninger er ikke bare et problem for forskere, det kan også få uheldige konsekvenser ved senere behandling av pasienten. Dette, sammen med den økte graden av rett til medbestemmelse som en slik kombinert modell innebærer, skulle tilsi at denne løsningen vil kunne ivareta den enkelte pasients interesser bedre enn den løsning som foreslås i rapporten *Gode helseregistre - bedre helse*.

En annen åpenbar fordel ved at alle feil korrigeres i journalene, er at opplysningene da vil være korrekte dersom disse på et senere tidspunkt skal avgis til et annet register eller til et forskningsprosjekt.

Ved bruk av TPF vil den foreslåtte løsningen gi en *teknisk mulighet* for å utlevere person-identifiserbare opplysninger fra helseregistrene. For å bidra til å sikre at denne muligheten ikke benyttes til andre formål enn det som er bestemt for det enkelte register, er det viktig at TPF opprettes som en tiltrodd tredjepart, uavhengig både av registrene og de som avgir opplysninger til registrene.

Ved å la en forespørsel om utlevering gå via TPF vil det også være teknisk mulig å foreta utlevering av opplysninger fra slike registre til helsepersonell som yter helsehjelp til

pasienten, uten at pasientens identitet gjøres kjent for registret. Enkelte av de nåværende sentrale helseregistrene, slik som SYSVAK, benyttes allerede til forebygging, behandling og oppfølging av den enkelte pasient. Denne typen mulighet som også er nevnt på side 104 i rapporten *Gode helseregistre - bedre helse*, vil altså også kunne realiseres for registre basert på en slik kombinert modell.

Tiltak mot bakveisidentifisering

Selv om den registrertes identitet blir kryptert, vil det fremdeles foreligge en reell fare for at enkelte registrertes identitet kan avsløres på grunnlag av opplysningene i et slikt register, såkalt "bakveisidentifisering". Faren for at en bestemt person skal kunne bakveisidentifiseres øker naturlig nok med mengden av opplysninger som er registrert om vedkommende.

Særlig opplysninger som også er finnes i offentlig tilgjengelige kilder, slik som fødselsdato, bostedskommune, yrke, stillingsbetegnelse og utdannelse, medfører stor fare for bakveisidentifisering. Men også "uskyldige" opplysninger om kontakter med helsevesenet som personer i bekjentskapskretsen ofte har kjennskap til, kan bidra til slik bakveis-identifisering.

Å vite at en kvinne med en bestemt alder som er bosatt i en liten kommune har daglig besøk av hjemmesykepleier og at vedkommende har hatt et rehabiliteringsopphold i et bestemt tidsrom, vil trolig være tilstrekkelig til å identifisere kvinnen i IPLOS, selv om dette er et pseudonymt register.

I de fleste tilfeller vil det å fjerne bostedskommune og alder være tilstrekkelig til at de registrerte blir anonyme. Som det også nevnes i rapporten, fjernes da også ofte slike opplysninger når datasett utleveres til forskere. For å minske faren for de som har direkte tilgang til opplysninger i et helseregister, kan foreta bakveisidentifisering, kan det vurderes å skille opplysninger som også er finnes i offentlig tilgjengelige kilder ut i et eget del-register. Dette registret kan så kobles med registre som inneholder helseopplysningene når det foreligger et legitimt behov.

Om tekniske løsninger

At det å realisere tekniske løsninger for håndtering av pseudonyme registre ikke vil være noe stort problem, understøttes av den rapporten som skrivegruppe for tekniske løsningskonsepter i forprosjekt for Nasjonalt helseregisterprosjekt har utarbeidet. Her heter det blant annet[3]:

> "Sett fra et teknisk ståsted er ikke forskjellen mellom løsningene for de tre registertypene [pseudonyme, personidentifiserbare med samtykke og personidentifiserbare uten samtykke] nødvendigvis store. Det gjelder både når det gjelder registrering, arbeid med opplysningene i registret og sammenstilling med opplysninger fra andre registre."

Ettersom et pseudonym er en kryptert identitet, bør det heller ikke være noen stor utfordring å utvikle de løsninger som er nødvendig for etablere helseregistre etter den type kombinert modell som beskrives i dette notatet. For å få et bedre grunnlag til å fatte beslutning når det

---

[3] Sitat fra kapittel *16.1 Pseudonymiseringsløsninger*. Rapporten finnes på http://www.kunnskapsnettverk.no/C15/C2/Nasjonalt%20Helseregisterprosjek/Document%20Library/Hoveddokument%20tekniske%20l%c3%b8sninger%20NHRP%20v1_1.pdf

gjelder den framtidige modellen for nasjonale helseregistre, bør det derfor vurderes å utrede denne typen alternativer nærmere.

Om kryptering av identitet i eksisterende registre

Stortinget har vedtatt at direkte personidentifiserende kjennetegn skal lagres kryptert i de registrene som er opprettet med hjemmel i helseregisterloven § 8 annet ledd, da med unntak av nasjonal database for elektroniske resepter. Dette innebærer at en for hvert enkelt av disse registrene må opprette en intern tjeneste for kryptering og dekryptering av identitet.

Selv om slik kryptering ennå ikke er etablert for alle registrene, må en kunne legge til grunn at alle registrene etter hvert vil rette seg etter loven.

Det finnes flere forskjellige metoder som kan benyttes ved kryptering av identitet. Hvilken av disse metodene som velges vil knapt være merkbare i forhold til de totale kostnadene ved etablering av en løsning for kryptering av identitet. Ved intern kryptering bør det derfor velges en krypteringsmetode som er sterk nok til at den kan oppfylle de krav som stilles til generering av pseudonym.

Teknisk sett vil det ikke være noen forskjell på en intern løsning for kryptering av identitet og en ekstern løsning som tilbyr de samme krypteringstjenestene. Dersom en forutsetter at registrene får en høyhastighets tilkobling til helsenettet, noe som uansett bør være en forutsetning for å kunne gå over fra papirbasert til elektronisk innrapportering til registrene, vil det heller ikke ytelsesmessig være mye å tjene på å ha en slik løsning internt i det enkelte register.

Selv om Stortinget har åpnet for at krypteringen kan skje internt, taler derfor mye for at nødvendige tjenester forbundet med kryptering av identitet bør etableres hos en ekstern aktør, som hvert enkelt register kan inngå avtale med.

Mens SSB er TPF for Reseptregistret, er Skattedirektoratet TPF for IPLOS. Ettersom de tjenester som er nødvendig for kryptering av identitet, har mye til felles med tilsvarende tjenester for pseudonymisering, bør det vurderes å opprette en felles TPF som kan tilby pseudonymiseringstjenester for eksisterende og nye pseudonyme registre, samtidig som det tilbys krypteringstjenester for øvrige helseregistre.

Som tidligere nevnt, benyttes enkelte av de eksisterende sentrale helseregistrene, slik som SYSVAK, allerede til forebygging, behandling og oppfølging av den enkelte pasient. Når disse registrene har lagt om til kryptert identitet slik som bestemt i helseregisterloven, vil en måtte endre de mekanismer som nå benyttes for å gi eksternt helsepersonell nødvendige opplysninger f.eks. om hvilke vaksinasjoner et barn har mottatt.

Den type funksjonalitet som da må utvikles, vil i utgangspunktet kunne benyttes i enhver situasjon hvor det foreligger et legitimt behov for tilgang til opplysninger om en bestemt pasient i et slikt register. Dette vil for eksempel kunne benyttes til å gi den enkelte registrerte selv i IPLOS, Reseptregistret, eventuelle nye pseudonyme registre eller registre med kryptert identitet. Slikt innsyn kan f.eks. tenkes gitt via en sikker løsning etablert på "Min side" slik som foreslått i tiltak 61 på side 127 i rapporten *Gode helseregistre - bedre helse*.

Også dette taler for at en velger en felles løsning ved kryptering av identitet i de eksisterende registrene. Å utvide en slik felles løsning med den funksjonalitet som er nødvendig for å realisere en kombinert modell slik som foreslått i dette notatet, bør ikke by på store problemer. Det er heller ingen grunn til å tro at de driftskostnader som er forbundet med en

slik felles løsning, vil bli særlig påvirket av om registrene er pseudonymiserte eller om identiteten er lagret kryptert.

Også ut fra et systemarkitektursynspunkt vil det være en klart bedre løsning å etablere fellestjenester som alle aktører får tilgang til, framfor å la de enkelte registrene håndtere det meste selv. Og dette vil være helt i tråd med gjeldende strategi for tjenesteorientert arkitektur i spesialisthelsetjenesten[4] hvor det er en klar målsetning at det på flere områder skal etableres fellestjenester som kan benyttes av alle helseforetak. Sett i forhold til de typer tjenester som vurderes etablert på andre områder, framstår de tjenester som er nødvendig for å håndtere en kombinert modell for helseregistre, verken som spesielt ressurskrevende eller tidskritiske.

[4] Tjenesteorientert arkitektur i spesialisthelsetjenesten. Hovedrapport – full versjon. Nasjonal IKT 2008