Nasjonalt senter for
e-helseforskning

NOTAT

Tromsø 23.09.2019

Svar på høringsnotat tilsendt i høringsbrev av 26.06.2019 om endringer i forskrift om Nasjonalt vaksinasjonsregister og forskrift om Meldingssystemet for smittsomme sykdommer (MSIS)

Dette notatet gjelder kun forslaget til MSIS forskrift. Denne er gjort med bakgrunn i erfaringene fra forskningsprosjektet «Snow-sykdomsovervåking» eller «Snow prosjektet» som har pågått siden 1 januar 2007. I gjennomgangen vil vi referere til tekst i høringsnotatet, med eksakt ordlyd og kopiere tekst fra den nye personvernforordningen. Dette for å øke lesbarheten og synliggjøre svakhetene ved forslaget til MSIS forskrift.

Til side 4 avsnitt 6:
«Både MSIS-forskriften og helseregisterloven tilfredsstiller kravene som fremgår av personvernforordningen. Eksempelvis er det regler som gir nødvendige personverngarantier, jf. personvernforordningen artikkel 89, for behandling av opplysninger i MSIS. Enhver som får adgang eller kjennskap til helseopplysninger har taushetsplikt, jf. helseregisterloven § 17.»

Personvernforordningen Artikkel 89 punkt 1 sier:
«Behandling for arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål skal omfattes av nødvendige garantier i samsvar med denne forordning for å sikre den registrertes rettigheter og friheter. Nevnte garantier skal sikre at det er innført tekniske og organisatoriske tiltak for særlig å sikre at prinsippet om dataminimering overholdes. Nevnte tiltak kan omfatte pseudonymisering, forutsatt at nevnte formål kan oppfylles på denne måten. Dersom nevnte formål kan oppfylles ved viderebehandling som ikke gjør det mulig eller ikke lenger gjør det mulig å identifisere de registrerte, skal formålene oppfylles på denne måten.»

Dersom en skal følge prinsippet om at tekniske og organisatoriske tiltak som sikrer dataminimering er iverksatt kan en ikke sende informasjon til FHI. Det er full mulig å oppnå formålene til MSIS uten å sende sensitiv informasjon til FHI og uten å bruke direkte personidentifiserende informasjon, som vil innebære å ivareta dataminimering. Se flere detaljer nedenfor. MSIS-forskriften tilfredsstiller derfor ikke kravene som fremgår av personvernforordningen artikkel 89 punkt 1. Artikkel 89 nr 1 (siste setning) pålegger oss derimot å realisere løsninger slik at det ikke er mulig å identifisere de registrerte, slik Snow prosjektet har gjort.

Til side 4 avsnitt 6:
«Dette kravet innebærer å begrense mengden innsamlede personopplysninger til det som er nødvendig for å realisere formålet.»

Det vil ikke være nødvending å kopiere og flytte individ data til FHI for å oppnå formålene med MSIS. Dette har vært demonstrert over mange år, siden 2010, gjennom pilotdrift av Snow sykdomsovervåkningssystem i Helse Nord og i Helse Midt.

Til side 4 avsnitt 6:
«Videre skal Folkehelseinstituttet, som dataansvarlig for MSIS, gjennomføre tekniske og organisatoriske tiltak for oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen, ifølge personvernforordningen artikkel 32 og helseregisterloven § 21.»

Artikkel 32 i personvernforordningen:
«Artikkel 32 Sikkerhet ved behandlingen

1. Idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene og behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige og databehandleren gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen, herunder blant annet, alt etter hva som er egnet,
    a) pseudonymisering og kryptering av personopplysninger,
    b) evne til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene og -tjenestene,
    c) evne til å gjenopprette tilgjengeligheten og tilgangen til personopplysninger i rett tid dersom det oppstår en fysisk eller teknisk hendelse,
    d) en prosess for regelmessig testing, analysering og vurdering av hvor effektive behandlingens tekniske og organisatoriske sikkerhetstiltak er.
2. Ved vurderingen av egnet sikkerhetsnivå skal det særlig tas hensyn til risikoene forbundet med behandlingen, særlig som følge av utilsiktet eller ulovlig tilintetgjøring, tap, endring eller ikke-autorisert utlevering av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet.
3. Overholdelse av godkjente atferdsnormer som nevnt i artikkel 40 eller en godkjent sertifiseringsmekanisme som nevnt i artikkel 42 kan brukes som en faktor for å påvise at kravene i nr. 1 i denne artikkel er oppfylt.
4. Den behandlingsansvarlige og databehandleren skal treffe tiltak for å sikre at enhver fysisk person som handler for den behandlingsansvarlige eller databehandleren, og som har tilgang til personopplysninger, behandler nevnte opplysninger bare etter instruks fra den behandlingsansvarlige, med mindre unionsretten eller medlemsstatenes nasjonale rett krever at vedkommende gjør dette.»

Snow systemet, som allerede er i drift i deler av landet, har demonstrert at en kan ivareta formålene med MSIS uten å utsette samfunnet vårt for kostnadene rettet mot tiltak for å ivareta informasjonssikkerhet og uten å utsette pasientene for økt risiko for eksponering av helseinformasjon av ekstremt sensitiv art.

Dersom en tar hensyn til hva som er teknisk mulig i dag, slik artikkel 32 punkt 1 nevner, så er det ikke lenger behov for å kopiere og flytte individ data til FHI for å oppnå formålene med MSIS. Alle formålene med MSIS kan ivaretas ved hjelp av andre metoder enn de foreslåtte.

Det er også nødvendig å ta hensyn til endret risiko for brudd på pasientenes personvern. Det er ikke grunn til å tro at Norge er mindre utsatt for hacking enn andre nasjoner. Kopiering, lagring og prosessering av sensitiv informasjon på nye steder øker sannsynligheten for utilsiktet eksponering. Det øker også kostnadene. Sannsynligheten for brudd på personvernet til pasienter gjennom eksponering av innhold i pasient-journalinformasjon i USA har økt dramatisk de siste årene. Gjennom en studie gjennomført ved Nasjonalt senter for e-helseforskning i 2016 (Bellika JG, Makhlysheva A, Bakkevoll PA. A Significant Increase in The Risk for Exposure Of Health Information In The United States. Result from Analysing the US Data Breach Registry. :5.) ble det avdekket at sannsynligheten for et brudd på informasjonssikkerhet i USA økte fra 0,5 brudd pr dag i 2010 til 0,89 brudd pr dag i 2016. Så langt i år er det i USA registrert 332 brudd som omfatter helseinformasjon til 37,5 millioner amerikanere, altså flere enn et brudd pr dag. Forekomst av eksponering gjennom hacking av helse IT systemer ble 15 doblet, fra 16 tilfeller i 2010 til 240 tilfeller i 2016. I dag er helseinformasjonen til mer enn 229 millioner (70%) av amerikanere eksponert gjennom brudd på informasjonssikkerheten, de siste årene hovedsakelig gjennom hacking. Også i Norge har vi opplevd tilfeller av hacking av helse IT systemer, uten at en har klart å avdekke hvem som har stått bak disse. Studien som ble gjennomført i 2016 slår fast at trusselnivået og sannsynligheten for brudd på informasjonssikkerheten er mye høyere enn tidligere og at trenden har vært jevnt stigende risiko i mange år.

Med bakgrunnen i situasjonen beskrevet ovenfor vil foreslått løsning måtte innebære store kostnader til å ivareta informasjonssikkerheten. Disse kostnadene er unødvendige å påføre samfunnet vårt, siden formålene kan oppnås ved hjelp av andre metoder som ikke medfører ekstra kostnader til informasjonssikkerhetstiltak ut over de som allerede er iverksatt av helseforetakene og Norsk Helsenett. Ressursene kan, med bruk av andre metoder, i stedet brukes på andre oppgaver enn å ivareta informasjonssikkerhet, for eksempel å ivareta formålene med MSIS.

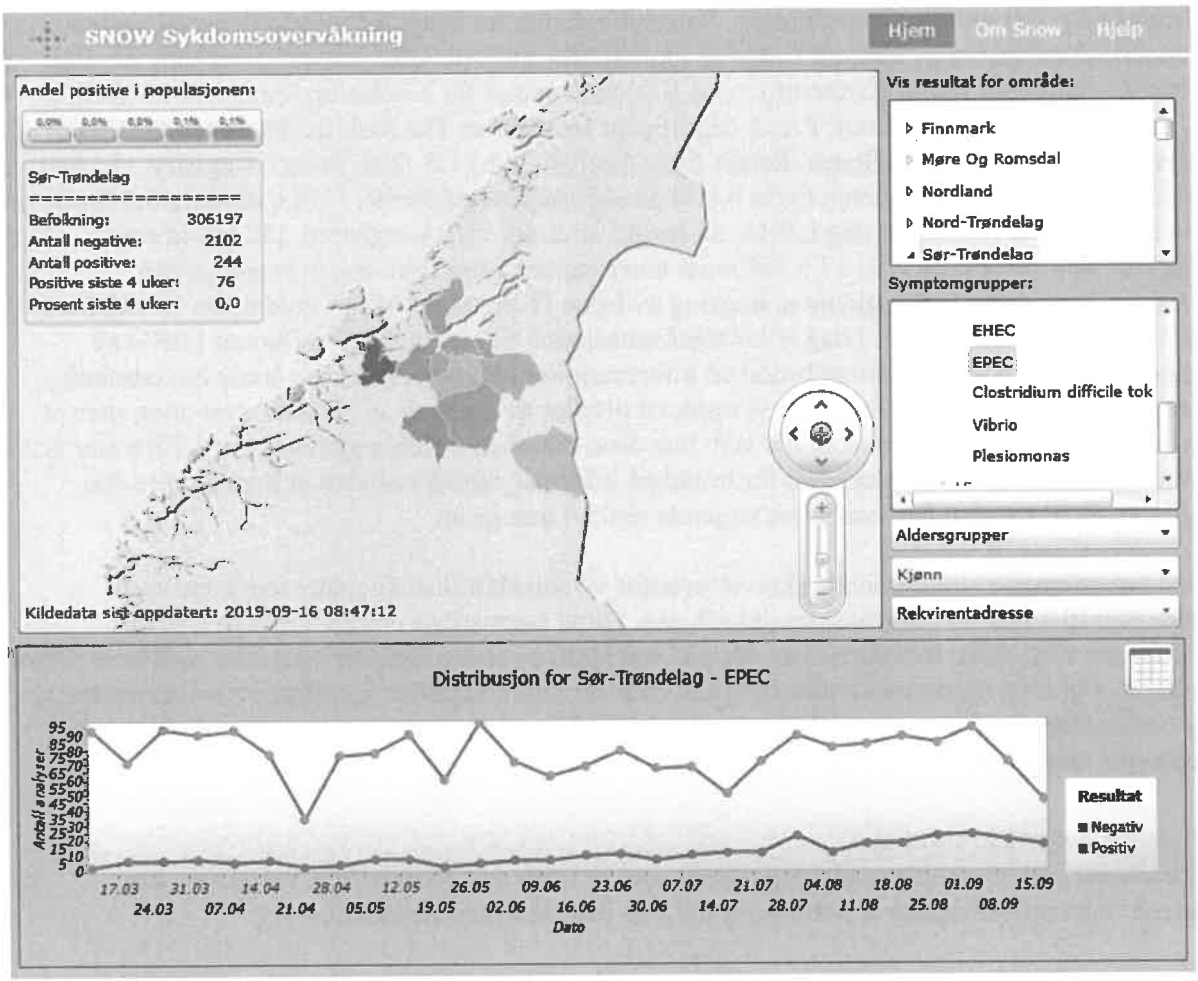
Til side 5 avsnitt 2, setning 5:
«Registeret kan inneholde opplysningstyper som er listet opp i forskriften, men kun i den utstrekning opplysningene er nødvendig for å nå formålet med registeret.»

Snow prosjektet har demonstrert at det ikke er nødvendig å distribuere sensitiv pasientinformasjon ut av mikrobiologilaboratoriene for å oppnå formålene med registeret.

Til side 10, avsnitt 1:
«Dagens system gir ikke kunnskap om hvor mange personer som blir testet for de ulike sykdommene og hvilke sykdommer det testes for. Det er behov for kunnskap om hvor stor andel positive tester utgjør av det totale antallet tester som utføres for å kunne ha tilstrekkelig kunnskap om utbredelsen av smitte, omfanget av testing og kvaliteten på testene. Positive prøvesvar for sykdommene som fremgår i vedlegg I, vil inngå i registeret på samme måte som i dag, mens for de øvrige prøvesvarene vurderer departementet at de direkte personidentifiserende kjennetegn

ikke er nødvendig å lagre og skal dermed slettes så raskt som mulig i en automatisk prosess etter kvalitetssikring.»

Snow sykdomsovervåking som er i bruk i Helse Nord og Helse Midt publiserer hver dag oversikt over hvor mange personer som blir testet for de ulike sykdommene og hvilke sykdommer det testes for. Se skjermdump av denne informasjonen nedenfor. Denne informasjonen har vært tilgjengelig online i mange år.



Figur 1. Distribusjon av negative og positive EPEC prøver i Sør-Trøndelag mandag 16 september.

Vår erfaring er at kvalitetssikringen av prøvesvar, utført ved andre laboratorier, kan endre endelig svar på prøve opp til 90 dager etter analysedato. En må derfor beholde identiteten til pasienten like lenge før negative prøvesvar kan de-identifiseres. Å oppbevare identiteten til pasienter i mange dager for negative prøvesvar for seksuelt overførbare sykdommer i et nasjonalt register, vil ikke legge begrensninger på interessen fra hackere til å bruke disse dataene til utpressing. For positive prøvesvar på seksuelt overførbare sykdommer vil ikke interessen være mindre. Det siste året har det vært en økende forekomst av utpressing via email. Frykten for at noen skal få tak i

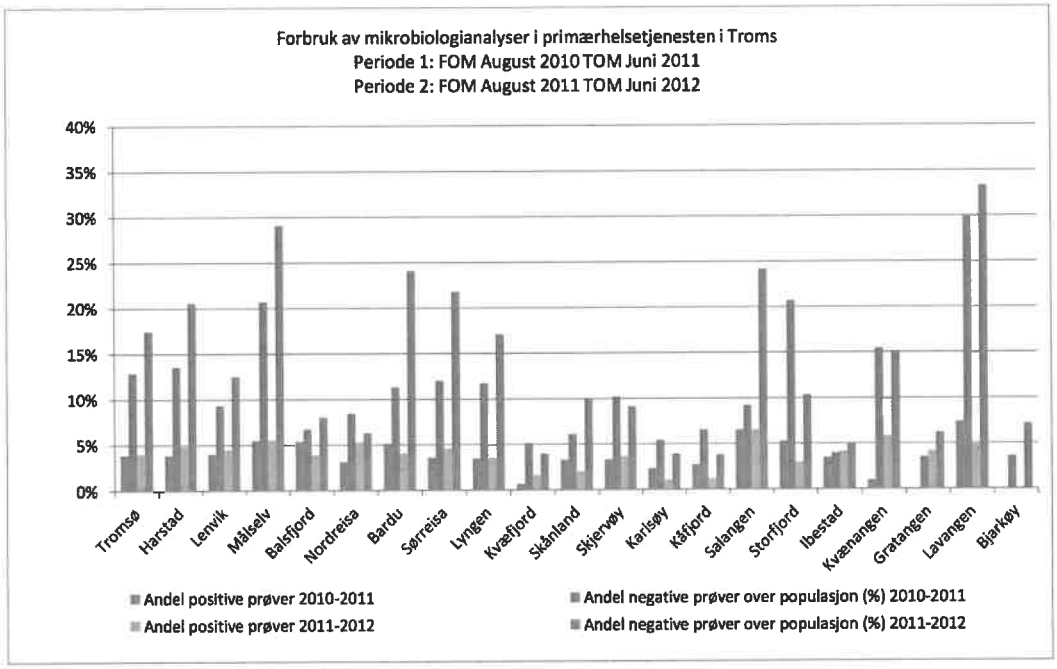
slik informasjon via hacking alene, kan få utsatte til å avstå fra nødvendig testing, og de negative konsekvensene dette har.

Til side 10, avsnitt 2:
«Forslaget videreutvikler dagens system for innmelding av smittsomme sykdommer. Gode data om smittsomme sykdommer er viktig for forebygging og bedre beredskap mot utbrudd av smittsomme sykdommer, økt pasientsikkerhet og bedre kvalitet på helse- og omsorgstjenester. Det er behov for kunnskap om hvor mange og hvilke tester som tas nasjonalt. I MSIS er det opparbeidet erfaring og ekspertise om utbredelsen av smittsomme sykdommer og departementet vurderer at en sentral oversikt over testomfanget vil gi nødvendig kunnskap om utbredelsen av smittsomme sykdommer i samfunnet og gi et bedre smittevern totalt sett. Mer kunnskap vil gi mulighet for ytterligere forebygging og målretting av tiltak.»

Vi er enige i at gode data er nødvendig for forebygging og beredskap mot utbrudd av smittsomme sykdommer, økt pasientsikkerhet og bedre kvalitet på helse- og omsorgstjenester. Aktivitetene som gjennomføres for å nå disse målene foregår imidlertid ikke sentralt, men i hver helseinstitusjon og helseregion, og gjennom beslutningene helsearbeidere tar. En bør derfor bruke ressursene på å styrke alle nivå, også sentralt, for å oppnå målene. Løsningen som her er foreslått vil imidlertid måtte tilføre mange ressurser for å ivareta IT løsningen og informasjonssikkerheten.

Til side 10, avsnitt 3:
«Departementet legger vekt på at en sentral begrunnelse for forslaget er det vil gi nødvendig kunnskap om i hvilken grad økninger eller utbrudd av smittsomme sykdommer skyldes reelle forhold eller om årsaken er økning i testaktiviteten. Forslaget vil også kunne gi bedre kunnskap om antibiotikaresistens og bærerskap av smittestoff for sykdommer som er meldingspliktig, jf. vedlegg 1 i forskriften.»

Snow sykdomsovervåkning som er i drift i Helse Nord og Helse Midt kan allerede avdekke om økt forekomst skyldes økt testing eller økt forekomst. NSE´s erfaring, etter mange års drift av sykdomsovervåkningstjenesten, er at det er veldig stor variasjon i testpraksis blant primærleger. Se Figur 2 nedenfor. Mens noen kommuner har et aktivt testmønsteret, for nettopp å overvåke forekomst, tester legene i andre kommuner ikke i samme omfang. Mulighetene til å oppdage utbrudd er derfor i mye større grad avhengig av legenes testpraksis enn av løsningen som her foreslås. En bør derfor bruke ressurser på å harmonisere testpraksis blant leger, slik at en styrker mulighetene for deteksjon og prediksjon av utbrudd. En er ikke avhengig av foreslåtte løsning for å kunne konstatere om årsak til økning skyldes reelle forhold eller økt testpraksis som vist i Figur 1 ovenfor.



Figur 2. Variasjon i testpraksis i Troms i årene 2010 til 2012.

Til side 10, avsnitt 4, setning 6:
«Den andre gruppen utgjør prøvesvar for alle andre sykdommer som ikke er fremgår av vedlegg I og negative prøvesvar, og som kun skal telles summarisk og derettter slettes.»

Dersom en skal oppnå korrekte tall vil det være nødvendig å oppbevare de opprinnelige test dataen en periode (opp til 90 dager) for å sikre at kvalitetssikringen av prøvesvarene kan endre endelig prøveresultat.

Side 10, avsnitt 6:
«Departementet mener at elektronisk innmelding av samtlige prøvesvar vil kunne gi et løft for smittevernet i Norge, en bedre beredskap mot antibiotikaresistens og et betydelig mer effektivt system for innrapportering av laboratorieresultater til MSIS. Tiltaket er også et godt eksempel på økt digitalisering. Departementet mener at den helsefaglige og samfunnsmessige nytten av registeret klart overstiger personvernulempene.»

Det er fullt mulig å skape et løft for smittevernet uten personvern-ulempene forslaget innebærer. Det finnes allerede et effektivt system for gjenbruk av laboratorieresultater i drift. Dette systemet heter Snow systemet og dekker i dag laboratoriene i 2 av 4 helseregioner og har vært i drift siden 2010. Skjermbilde fra informasjonssystemet er vist i Figur 1. Å ta i bruk den eksisterende alternative løsning vil også innebære en økt digitalisering, men også innovasjon da nye teknologisk muligheter tas i bruk nasjonalt. Det er fullt mulig å oppnå den samme nytten uten personvernulempene og kostnadene som en legger opp til i dette forslaget. Det er derfor uforståelig hvorfor en skal utsette pasienten for personvernulempene når bedre og billigere alternativer eksisterer og er i drift.

Til seksjon 3.2.1, avsnitt 1:
«Laboratoriene melder i dag ikke ved negative testresultater og vi mangler derfor oversikt over det totale antall tester som gjennomføres. Kunnskap om omfanget av negative prøvesvar er nødvendig blant annet for å kunne skille mellom variasjoner i sykdomsforekomst og variasjoner i testaktivitet. Vi har per i dag ikke oversikt over hvorvidt økte innrapporteringer til MSIS-registeret skyldes faktisk økning i antall smittede eller om det kun er et resultat av at det er gjennomført flere tester.»

Til setning 1:
Snow system teller i dag opp totalt antall tester og publiserer dette på internett daglig, se Figur 1.
Til setning 2:
Dette er allerede mulig å gjøre med Snow systemet.
Til setning 3:
Dette kan vi allerede gjøre med Snow systemet. Se Figur 1.

Til seksjon 3.2.1, avsnitt 2, setning 4:
«Det er 21 laboratorier i medisinsk mikrobiologi som kun har lokal oversikt over tester og forekomst av sykdommer som diagnostiseres i det enkelte laboratorium, men det finnes ingen samlet nasjonal oversikt over testvirksomhet og -resultater.»

Dette stemmer ikke. De 7 laboratoriene som dekkes av Snow systemet har komplett oversikt over test virksomheten og forekomsten av smittsomme sykdommer i Helse Nord og Helse Midt.

Til seksjon 3.2.1, avsnitt 2, setning 6:
«Som en konsekvens av dette er kunnskapen om forekomst av smittsomme sykdommer i samfunnet begrenset og det er vanskelig å vurdere om det er faktiske endringer i sykdomsforekomst eller om det eksempelvis er forhold i laboratoriene som skaper endringer.»

For laboratoriene og områdene som dekkes av Snow systemet mottar sykehusleger, smittevernleger, fastleger, kommuneleger og andre hver uke oversikt over forekomst av smittsomme sykdommer på email. Kombinert med informasjonssystemet vist i Figur 1 er det fullt mulig å fastslå om endringer skyldes endret testpraksis eller endret forekomst.

Til seksjon 3.2.2, avsnitt 1:
«Elektronisk innmelding av opplysninger til MSIS fra laboratoriene på samme format som til legen som har bestilt prøven, vil kunne gi raskere og mer effektiv kunnskap om smittsomme sykdommer og antimikrobiellresistens. Det vil også kunne medføre en ressursbesparelse både i laboratoriene og ved Folkehelseinstituttet.»

Denne innsparingen kan potensielt raskt spises opp av tiltakene for å sikre personvernet til pasientene. Veldig strenge sikringstiltak må iverksettes for å beskytte ekstremt sensitivt informasjon. Dersom en benytter løsninger som ligner på Snow løsningen, trenger en ikke like

store sikringstiltak ut over de helseforetakene allerede har iverksatt for å ivareta informasjonssikkerheten i laboratoriesystemene. Med begrensede ressurser er det derfor mer fornuftig å bruke ressursene på analyse og forskning, som er formålet med MSIS, heller enn å lage løsninger (som også er kostnadskrevende) som øker risikoen for brudd på personvernet.

Til seksjon 3.2.3, avsnitt 1:
«Forslaget går ut på at prøvesvar fra laboratoriene skal sendes til Folkehelseinstituttet i en kryptert forsendelse for registrering og kvalitetssikring. Deretter skal direkte identifiserende kjennetegn slettes, med mindre meldingen gjelder sykdommer som fremgår av vedlegg 1 til forskriften. Direkte identifiserende kjennetegn (fødselsnummer) er nødvendig ved innmelding av prøvesvarene av hensyn til å unngå dobbelmeldinger og for å kunne gjennomføre nødvendig kvalitetssikring.»

Sletting av identifiserende informasjon vil medføre at antall tilfeller blir feil. Legekontor som benytter forskjellige laboratorier, for eksempel i oppfølgingsprøver, vil ikke kunne identifiseres. I et forsøk på distribuert de-duplisering av prøvesvar mellom UNN, St-Olavs og Fürst fant vi ca. 400 prøver på de samme personene. Det er ikke nødvendig å bruk fødselsnummer for å oppdage dobbeltmeldinger(duplikater og gjentatte tester). I en studie fullført i 2017 (ref Yigzaw KY, Michalas A, Bellika JG. Secure and scalable deduplication of horizontally partitioned health data for privacy-preserving distributed statistical computation. BMC Med Inform Decis Mak. 2017 Jan 3;17(1):1), gjennomførte vi et slikt eksperiment. I eksperimentet identifiserte vi duplikate tester på tvers av 3 mikrobiologilaboratorier (UNN, St- Olavs og Fürst). De-dupliseringsprosessen ble gjennomført på 22 sekunder.

Til side 14, avsnitt 1, setning 3:
«Departementet understreker at det kun er nødvendige og relevante opplysninger om hvert enkelt tilfelle som registreres og behandles, noe som er i tråd med det grunnleggende kravet om dataminimering.»

Når det finnes alternative løsninger som ikke krever lagring av personnummer eller overføring av svært sensitive personopplysninger til et nasjonalt mottak kan forslaget IKKE karakteriseres å ivareta dataminimering. I EUs veiledning til personvernkonsekvensvurdering (Data Protection Impact Assessment (DPIA)) anbefales at dataansvarlig både før, under design av løsning, og kontinuerlig ved bruk av løsning vurderer den løpende risikoen. I henhold til denne veilederen karakteriseres løsninger som prosesserer store mengder helseinformasjon som «likely to result in high risk». Informasjonen i denne løsningen må karakteriseres som svært sensitiv og ettertraktet av hackere med utpressing som mål. Løsningen som her foreslås burde derfor vært gjenstand for diskusjoner om alternative design av løsning. En slik diskusjon ville sannsynligvis resultert i løsningsforslag der risiko for pasientenes personvern ville vært lavere enn i det foreliggende forslag til løsning.

Til side 14, avsnitt 2, setning 3:
«Det kan oppleves som en ulempe for den enkelte registrerte at opplysninger om prøveresultater behandles uten samtykke og mulighet for reservasjon.»

Rapportering av enkelte analyseresultat, som for eksempel negative og positive prøvesvar om seksuelt overførbare sykdommer, vil åpenbart kunne oppleves som en ulempe, spesielt siden disse opplysningene vil være ettertraktet av hackere med intensjon om å bruke slike opplysninger til utpressing. Forekomst av hacking av helsesystemer har vært økende det siste tiåret. I USA, som har et offentlig register over brudd på personvernbestemmelsene der brudd på personvernet skal rapporteres, viser oversikten at 229 millioner av befolkningen i USA har fått sine helseopplysninger eksponert som følge av ulike typer brudd. Det er en klar overvekt i forekomst av hacking som årsak til eksponering av sensitive helseopplysninger. Sett i lys av at alternative løsninger, som innebærer mindre risiko eksisterer, er i bruk, og ikke har samme behov for å etablere rigide systemer som ivaretar informasjonssikkerhet ut over de vi allerede har etablert, vil dette forslaget, om det gjennomføres, helt klart kunne oppleves som en *unødvendig* og *kostbar* ulempe og en belastning for pasientene.

Til side 14, avsnitt 2, setning 4:
«Begrunnelsen for innmelding av opplysninger uten reservasjonsrett og samtykke er at det er nødvendig med komplette datasett.»

Snow systemet, som er i drift i dag i 2 helseregioner, har demonstrert at innrapportering av opplysninger til et sentralt register ikke er nødvendig for å ivareta formålene. En trenger ikke å registrere opplysninger om pasienten andre steder enn i LIS systemene for å ivareta formålene med MSIS. Ved å benytte teknologi for distribuert data-analyse er det mulig å oppnå komplette datasett, uten innmelding til et sentralt register. En slik innmelding øker ikke bare nødvendig eksponering, men også sannsynligheten og konsekvensene av utilsiktet eksponering av ekstremt sensitive helseopplysninger.

Til side 14, avsnitt 2, setning 10:
«Nytteverdien og behovet for fullstendige data, er imidlertid større enn personvernulempene ved å fravike krav om samtykke og reservasjonsrett.»

Når alternative løsninger som ikke innebærer behov for å overføre sensitiv informasjon til et sentralt register eksisterer, og det er mulig å unngå personvernulempene, bør en ikke fravike kravene til samtykke og reservasjonsrett.

Side 14, avsnitt 6:
«Personvernregelverket forutsetter at sikringstiltakene er tilpasset opplysningenes art, omfang, behandlingsformål og behandlingskontekst. Det skal tas hensyn til både sannsynlighet for og konsekvens av eventuelle brudd på sikkerheten når sikringstiltak velges.»

Sikringstiltakene for å ivareta informasjonssikkerheten til et nasjonalt system med svært sensitiv informasjon vil nødvendigvis måtte være svært omfattende og kostbare. Alle disse sikringstiltakene vil komme i tillegg til tilsvarende sikringstiltak som allerede eksisterer i helseforetakene som drifter LIS systemene. Siden det eksisterer en alternative løsning, som ikke trenger å etablere like omfattende sikringstiltak ut over det som helseforetakene allerede har etablert, fremstår foreslått løsningen som unødvendig bruk av knappe økonomiske ressurser.

Nasjonalt senter for
e-helseforskning

NOTAT

Seksjon 3.4.2, avsnitt 3, setning 3:
«Reservasjonsrett vil medføre at ikke alle hendelsene meldes inn til MSIS og dermed at opplysningene ikke blir komplette, noe som eksempelvis kan medføre at råd gis på feil grunnlag»

Komplette data i et overvåkningssystem kan oppnås uten innrapportering, som demonstrert av Snow systemet.

Til seksjon 3.4.3, avsnitt 2:
«Departementet vurderer at opplysningene må lagres på samme som måte som øvrige sykdommer i MSIS. Opplysningene i MSIS-registeret skal lagres i ubegrenset tid for å kunne se utvikling over tid og ha mulighet til å avdekke sammenhenger vi ikke har kunnskap om i dag.»

En vil kunne oppnå samme formål med lagring av opplysningene i ubegrenset tid i LIS systemene.

Til kapittel 4, avsnitt 3:
«Forslaget om innmelding av mikrobiologiske laboratoriefunn til MSIS dekkes innenfor gjeldende budsjettramme.»

Å overføre positive og negative prøvesvar fra mikrobiologilaboratorium til FHI bør, om den gjennomføres, innebære en styrking av rutiner og systemer knyttet til informasjonssikkerhet. MSIS registeret vil fremstå som en honningkrukke for hackere med et stort potensiale for utpressing.

Oppsummering
Oppsummert fremstår forslaget som ikke tilstrekkelig gjennomtenkt med hensyn til personvernkonsekvensene og kostnadene som er nødvendig for å beskytte informasjonen. En bør diskutere andre løsninger der disse svakhetene rettes opp, slik EUs veiledning til personvernkonsekvensvurdering anbefaler. Samtidig støtter vi målsetningen om å styrke smittevernet, men dette bør gjøres på alle nivå. Ved å unngå kostnadene som følger av nødvendige informasjonssikkerhetstiltak ved foreslåtte løsning, kan en styrke kapasiteten til analyse og forskning.

Med vennlig hilsen

Johan Gustav Bellika

Prosjektleder for Snow sykdomsovervåking

Professor ved Nasjonalt senter for e-helseforskning
Professor II ved Institutt for klinisk medisin, Helsevitenskapelig fakultet, UiT Norges Arktiske Universitet