

# NOTAT

## Kommuners tilkobling til helsenett - sikkerhet

**Dette notatet tar for seg kommuners tilknytting til helsenettene og utfordringer knyttet til dette. Det gir en kort oversikt over status for noen regioner, samt beskriver utfordringer, særlig knyttet til sikkerhet.**

### 1. Status

Kort om status i en del av helseregionene:

Sør-Norsk Helsenett: Har foreløpig fokus på primærleger, spesialister og private aktører. Har ennå ikke konkret tilbud/løsning for kommunene.

Nord-Norsk Helsenett: Leverer primært tjenester direkte til helseinstitusjoner, f.eks. direkte til et sykehjem. Se også Alta-løsningen under løsningsalternativ.

Fra andre regioner har det foreløpig ikke kommet svar, men det er kjent at Midt-Norsk helsenett har gjort arbeid på området, bl.a. med utgangspunkt i løsninger skissert i Alta-rapporten.

### 2. Alta-løsningen

Så langt ser premissene lagt i Alta-prosjektet ut til å være førende for de helsenett som har gjort arbeid ift. kommunesektoren.

Hovedprinsippene i Alta-løsningen – beskrevet i rapporten ”Tilkobling til helsenett i Alta” er:

- Kommunen etablerer sonestruktur med intern og sikker sone
- Kommunen kobles direkte til helsenettet via indre sikkerhetsbarriere, ikke ved hjelp av Internett som transportvei
- Kommunen har eventuelt egen oppkobling til Internett
- Det installeres en VPN-terminator ved hver kommune for kryptering/dekryptering av data til og fra helsenettet.
- Det benyttes VPN-forbindelser for utveksling av informasjon mellom lokale posttjenere i de ulike kommunenes sikre soner
- Terminalserverløsninger benyttes opp mot sentrale systemer for å differensiere sensitive personopplysninger fra kommunens øvrige data.

Valg av kobling direkte mellom helsenett og kommuner ble begrunnet med det økte sikkerhetsbidraget dette gir bl.a. ift beskyttelse mot inntregning, både for kommunen og helsenettet. En direktekobling vil også bedre kunne sikre tjenestekvalitet som vil være nødvendig for mer avanserte telemedisinske løsninger og videokonferanser. Å knytte helsenettet direkte til den indre sonen ble også vurdert til å ha en fordel ved at all trafikk inn til sikker sone vil være kryptert helt fram til sonen framfor å dekrypteres i ytre sikkerhetsbarriere

### **3. utfordringer**

Å knytte kommunale tjenester til helsenettet medfører en rekke utfordringer både tekniske og organisatorisk som krever gjennomtenkte og fleksible løsninger. Løsningene må være fleksible nok til å håndtere ulik organisering av kommunenes IT-drift, store variasjoner i kommunenes infrastruktur og IT-tjenester samt variasjoner i både størrelse og geografisk omfang.

#### **3.1. Sikkerhetsorganisasjon i kommunene**

Rapporten ”Tilkobling til helsenett i Alta kommune” samt forprosjektet for helsenetttilknytting i Alta og Bærum understreker behovet for en fungerende sikkerhetsorganisasjon i kommunen som skal tilknyttes helsenettet.

Krav til sikkerhetsorganisasjon finnes bl.a. i Personopplysningsloven og forskrift til denne, og kravene gjelder selv om kommunene har tilknytting til helsenett eller ikke. Likevel antas status på sikkerhetsorganiseringen hos kommunene å være høyst variabel, og selv i kommuner m. relativt høyt fokus på sikkerhet sentralt vil status for de aktuelle enhetene i helse- og pleie- og omsorgstjenesten kunne være lavere.

I Altaprojektet ble det vektlagt en grundig prosess for å øke sikkerhetsbevissthet og skape forankring for sikkerhetsledelsen og sikkerhetsorganisasjonen i helse- og sosialsektoren i Alta. Arbeidet innebar bl.a. gjennomføring av risikovurderinger, oversikt over IT-systemene i sektoren og etablering av rutiner for informasjonsbehandlingen. Det ble videre gjennomført to workshops m. deltakelse fra ledelse i helse- og sosialsektoren.

Kommuner som skal koble seg til helsenettet i framtiden bør pålegges å kunne dokumentere sitt styringssystem for informasjonssikkerhet. Viktigheten av at styringssystemet har en forankring i helse- og sosialsektoren bør understrekes.

#### **3.2. Ende- til ende ytelse**

Enkelte aktuelle anvendelser av helsenettet, særlig bruk av video, vil stille spesielle krav til tilknytningen, både ift. kapasitet og kvalitet. Videooverføring og spesielt videokonferanser stiller store krav til båndbredde, forsinkelse og graden av forstyrrelser i nettet. Båndbredden må både være relativt høy samt ha en jevn kvalitet, dvs. at linja har en garantert tjenestekvalitet. For å oppnå kortest mulig forsinkelse på signalet bør også datapakkene gå kortest mulig rute mellom avsender og mottaker.

Ved tilknytting av eksterne virksomheter til helsenettet er dette faktorer som bør tas i betraktning ved valg av løsning.

### **3.3. Sikre tjenester**

Klare løsninger for sikker ustrukturert kommunikasjon mellom helsepersonell er ennå ikke etablert i særlig omfang. Noen løsninger som kan være aktuelle er:

- Kryptert e-post: Kryptert e-post basert på en eller annen form for PKI-løsning, f.eks. Rammeavtale for PKI i helsevesenet, gjerne kombinert med andre sikkerhetsløsninger, f.eks. for å beskytte mot utilsiktet utlevering, feiladressering av e-post osv.
- Meldingsbasert dialog: Løsninger for kommunikasjon mellom helsepersonell som er integrert i fagapplikasjonene, f.eks. de respektive journalsystemene.

Begge disse løsningene har ulike fordeler og ulemper:

- Epost-løsningen kan være relativt enkel å få i drift
- Store deler av potensielle brukergrupper vil ha en eller annen form for erfaring med bruk av e-post
- Meldingsbasert dialog sikrer bedre at behovet for dokumentasjon ift. kommunikasjon om pasienter blir ivaretatt i og med at hver melding knyttes til den aktuelle pasienten.
- Meldingsbasert dialog

Generelt sett er forholdet til dokumentasjonsplikten en utfordring ift. elektroniske løsninger for uformell kommunikasjon om pasienter. Det eksisterer en rekke formål hvor denne type kommunikasjon vil være både nyttig og effektiv så lenge krav til sikkerhet er ivaretatt. Den beste løsningen vil være en løsning som sikrer at dokumentasjonsbehovet ivaretas samtidig som muligheten for kommunikasjon med alle nødvendige parter sikres.

### **3.4. utfordringer for helsenettene**

En sentral utfordring for helsenettene vil være kontroll m. trafikk internt i kommunen. Kommunen har et stort behov for kommunikasjon internt, som mot egne økonomi- og driftssystemer. Samtidig skal helse-institusjoner, som sykehjem, hjemme-tjenester osv. ha tilgang til informasjon, meldinger og kommunikasjon via helsenettet.

Typisk består en kommunes sikre sone også av en rekke etater som ikke er knyttet til helse, som sosial-etat, pp-tjeneste, evt. skole. Alle har potensielle behov for å nå kommunale felles-tjenester. utfordringen blir å beskytte koblingen mot helsenettet mot tilsiktet eller utilsiktet uautorisert trafikk fra kommunens sikre sone samtidig som kommunenes legitime kommunikasjonbehov internt kan ivaretas.

### **3.5. Annet**

Igangsetting av sikkerhetsarbeid, særlig i de mindre kommunene, vil være en utfordring både ift. kompetanse og ressurser. Erfaring tilsier at enkeltprosjekter settes i gang, kanskje begrunnet i mulig besøk av Datatilsynet eller på bakgrunn av innsalg fra konsulenter. Prosjektene får da gjerne kort varighet og resultater tas i liten grad inn i

kommunens daglige arbeide, verken i form av at rutiner praktiseres eller at sikkerhetsarbeid som metode, med gjennomføring av risikovurderinger, revisjon og oppfølging praktiseres.

Risikovurderinger som metode er et sentralt verktøy, både ift. lovkrav og som dokumentasjonsmåte og arbeidsprosess ift. sikkerhetsarbeid i kommunen. Kompetanse på dette området er sentralt, og bevissthet om metode, kompetansekrav osv. bør gjøres tilgjengelig for ansvarlige parter i kommunene.

Brukerbevisstgjøring vil også være en sentral utfordring. Særlig i kommunal pleie- og omsorgssektor kan det antas at IT-kompetanse, og dermed også kunnskap om trusler og problemstillinger knyttet til IT og informasjonssikkerhet er lav. Det bør derfor også vurderes tiltak for å nå denne brukergruppen med kompetansehevende tiltak.