

Sikkerhet, kommuner og helsenett.

Forprosjekt for
løsningsspesifikasjon for
tilkobling av Alta og Bærum
kommuner til helsenett

Versjon 2.0
Dato (21. juni 2002)

KITH Rapport 10/2002
ISBN 82-7846-134-1

KITH-rapport

Tittel

Sikkerhet, kommuner og helsenett

Forprosjekt for løsningsspesifikasjon for tilkobling av Alta og Bærum kommuner til helsenett.

Forfatter(e)

Tormod Hofstad

Arnstein Vestad

Olaf Trygve Berglihn

Oppdragsgiver(e)

Sosial- og helsedirektoratet

KITH

Kompetansesenter for IT i helsevesenet AS

Postadresse

**Sukkerhuset
7489 Trondheim**

Besøksadresse

Sverresgt 15, inng G

Telefon

73 59 86 00

Telefaks

73 59 86 11

e-post

firmapost@kith.no

Foretaksnummer

959 925 496

Rapportnummer

KITH-Rapp10/02

URL

<http://www.kith.no/arkiv/rapporter/nr102002.pdf>

Prosjektkode

SHdir-SKN02

ISBN

82-7846-134-1

Dato

27. juni 2002

Antall sider

48

Kvalitetssikret av

Bjarte Aksnes

Gradering:

Ingen

Godkjent av

Jacob Hygen
Adm. direktør

Sammendrag

Rapporten vurderer ulike alternativer og foreslår konkret løsning for tilkobling av pleie- og omsorgstjenesten i Alta og Bærum kommune til sine respektive regionale helsenett.

Løsningene bygger på følgende anbefalinger:

- 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.

I vedleggs form finnes Plan for hovedprosjekt, Sentrale ord og uttrykk, Prosjektdirektiv og Spørreskjema.

Forord

Å koble kommunenes helse- og omsorgstjeneste til regionale helsenett vil være et positivt bidrag til utviklingen av et godt og funksjonelt helsenett. Oppgaven med å foreslå en konkret måte å gjøre dette på har betydd avveininger mellom flere hensyn og har krevd at en har gjort forutsetninger i forhold til framtidige løsninger i helsenettet. Vi håper at rapportens forslag likevel oppfattes som et konstruktivt bidrag både av oppdragsgiver Sosial- og Helsedirektoratet, Alta kommune, Bærum kommune, de regionale helsenettene og andre interesserte.

Vi vil gjerne også få takke for det vi har opplevd som et konstruktivt samarbeid med alle involverte. Spesielt vil vi trekke fram det gode samarbeidet med Eterra AS Trondheim ved Terje Barø.

Tormod Hofstad

Arnstein Vestad

Olaf Trygve Berglihn

Innhold

SAMMENDRAG.....	2
BAKGRUNN FOR PROSJEKTET	5
PROSJEKTET.....	8
PROBLEMSTILLING	10
OVERORDNET LØSNING.....	19
ALTA KOMMUNE	22
BÆRUM KOMMUNE	33
ORGANISERING AV INFORMASJONSSIKKERHETEN I ALTA KOMMUNE ...	42
PROSJEKTPLAN HOVEDPROSJEKT	49
SENTRALE BEGREPER.....	60
PROSJEKTDIREKTIV	68
INTERVJUGUIDE OG SPØRRESKJEMA	75

Sammendrag

Bakgrunn

Forprosjektet er gjennomført på oppdrag fra Sosial- og helsedirektoratet. Oppdraget var å foreslå en konkret løsningsspesifikasjon for tilkobling av Alta og Bærum kommuner til helsenett, samt utarbeide en plan for et hovedprosjekt for gjennomføring av løsningsforslagene. Det skulle også utarbeides eventuelle forslag til organisatoriske tiltak for informasjonssikkerhet i Alta kommune. Løsningene er ment å ha overføringsverdi til andre kommuner.

Kommunal pleie og omsorgstjeneste er en del av helsevesenet som vil kunne ha nytte av å kobles til helsenett. En har tatt utgangspunkt i pleie og omsorgstjenestens behov for kommunikasjon med sykehus og legekontorer. I dette prosjektet har en primært sett på løsninger for kommunalt tilkobling til helsenett, men det har i den sammenheng også vært nødvendig å belyse noen problemstillinger og løsninger internt i kommunene og i helsenettene.

Problemstillinger

Prosjektet må finne løsninger som ivaretar krav til både informasjonssikkerhet og funksjonalitet, og dette medfører avveininger mellom flere behov og målsettinger. I tillegg må en avklare hva som tilligger hhv kommunen og helsenettet av ansvar i forhold til løsningene som i utgangspunktet berører begge parter.

De tjenestemessige behovene i omsorgstjenesten som legges til grunn i prosjektet er i prioritert rekkefølge: sikker e-post, standardiserte meldinger, tilgang til helsenett for helserelatert informasjon og tilgang til intranett/intern sone for administrative systemer. Også andre behov nevnes av omsorgstjenesten som interessante på noe lenger sikt. Det er i løsningsforslagene tatt høyde for behovet for tilgang til både intern og sikker sone.

Det er vurdert to alternative tilkoblinger til helsenett: Tilkobling direkte til regionale helsenett og tilkobling til helsenett med Internett som bæretjeneste.

Legekontorer forutsettes å være egen virksomhet og ha egen tilkobling til helsenett.

Det er forutsatt at kommuner har en klar strategi for behandling av personopplysninger iht til POL og POF. Følgende sikkerhetsbehov legges til grunn: Konfidensialitet, Tilgjengelighet og Integritet.

Forslag til overordnet løsning

- 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.

Løsningsforslagene for Alta og Bærum bygger på disse punktene og er beskrevet i hvert sitt kapittel i rapporten. I Alta antydes en kostnad på de tekniske installasjonene på 97.500,- kr., mens Bærum får en utgift på tilsvarende 13.500,- kr. Forskjellen skyldes ulikt utgangspunkt knyttet til kommunens eget nettverk.

Informasjonssikkerheten i Alta kommune

Det anbefales Alta kommune å gjennomføre et prosjekt for å etablere en sikkerhetsorganisasjon og et styringssystem for informasjonssikkerhet. Det er innhentet prisoverslag på 50.000,- kr. for kjøp av rådgivningstjenester i tillegg til interne ressurser.

Forslag til prosjektplan hovedprosjekt

Hovedprosjektet tar utgangspunkt i forprosjektets løsningsforslag og avsluttes med testing av tilkoblingen til helsenett. Det vil da være klart for utprøving av f. eks meldingsutveksling eller andre tjenester over nett.

Hovedprosjektet organiseres i hovedsak som to selvstendige og parallelle prosesser for Alta og Bærum kommune. Hovedprosjektet skal, i tillegg til oppkobling til helsenett, levere erfaringsmateriale for bruk av andre kommuner, helsenett og overordnet myndighet. Prosjektet deles i tre faser og vil kunne gjennomføres på ca 26 prosjektuger pluss ferie og nødvendig tid til beslutninger.

Et hovedprosjekt kan gjennomføres med en samlet kostnad på 981.000,- kr. eks. MVA. Da fordeles dette med 500.875,- kr. til Alta kommune, 50.000,- kr. til informasjonssikkerhet i Alta kommune, 214.164,- til Bærum kommune og 216.821,- kr. til helsenett.

Det må taes forbehold om kostnadene da det i hovedprosjektets fase 1 må innhentes tilbud eller anbud både på utstyr og nødvendig arbeid, herunder prosjektstyring og utarbeidelse av erfaringsmateriale. Prisene er veiledende og ment kun som beslutningsgrunnlag for etablering av hovedprosjektet.

Bakgrunn for prosjektet

Kommunenes rolle i helsevesenet er betydelig, og helsenettene må tilby gode løsninger for tilkobling av omsorgstjeneste og kommunal helsetjeneste forøvrig. Sentrale ord, begreper og uttrykk er nærmere definert og beskrevet i vedlegg B.

Helsenett og kommunale nett.

Formålet med å etablere regionale helsenett er å etablere en sikker og formålstjenlig infrastruktur for elektronisk samhandling i helsevesenet. I tillegg skal en kunne tilby aktørene i helsevesenet tjenester over nettet som for eksempel telemedisinske tjenester, videobaserte tjenester, katalogtjenester og sikker tilgang til Internett. I definisjonen av helsevesenet inngår også den kommunale helse og omsorgstjenesten.

Helsenettene har til nå hatt størst fokus på å koble opp sykehus og primærlegetjenesten. Det vil fremover i økende grad være fokus på å inkludere hele kommunehelsetjenesten, som også inkluderer den kommunale omsorgstjenesten, både for å tilby en sikker infrastruktur og for å være premissgiver for tjenesteutvikling.

Mange kommuner har bygd opp interne nett som håndterer utveksling av alle typer informasjon. En må i utgangspunktet anta at kommunene har løst egen sikkerhetsproblematikk, men på forskjellige måter. Datatilsynet har i forhold til den gamle personregisterloven utarbeidet en veileder i informasjonssikkerhet for kommuner og fylkeskommuner.

Kommunalt ansvar.

I utgangspunktet er det kommunens (virksomhetens) ansvar å sørge for tilstrekkelig sikkerhet i egne systemer til at de kan kobles på helsenett. Hovedfokus i dette prosjektet er å finne løsninger på kommunikasjonen ut fra kommunen, ikke internt i kommunen. Kommunene er underlagt Forvaltingsloven, samt en del særlover (hjemler) som beskriver de behandlingsansvarlige og databehandlers oppgaver og rettigheter mht til bruk av elektroniske hjelpemidler (EDB-systemer).

Personopplysningsloven (som trådte i kraft 01.01. 2001) (POL), Lov om behandling av personopplysninger og dens forskrift, Forskrift til personopplysningsloven, (POF) beskriver de retningslinjer som er satt for behandling av personopplysninger. Dette gjelder også for behandling av sensitive personopplysninger.

Det er altså lite ønskelig at overordnet myndighet instruerer kommunene om hvordan de konkret skal løse den beskrevne problematikken. Det er likevel av interesse å vurdere sikkerhetsløsninger i helsenettet og internt i kommunen i sammenheng når en søker å nå målsettingen om å inkludere kommunal helse og omsorgstjeneste i helsenett. Dette vil gi verdifull innsikt både for kommunene selv, helseforetakene og andre aktører i det videre arbeidet med utvikling av helsenettet.

Sikkerhetsproblematikk.

Sikkerhetsproblematikk i forbindelse med bruk av IT-systemer i pleie- og omsorgstjenesten, relatert til tilkobling til helsenett, er et området som det har vært lite fokus på. En har god kjennskap til sikkerhetsproblematikk generelt i helsevesenet, men det har vært arbeidet lite innenfor dette tjenesteområdet. For å få et bedre grunnlag for å gå videre med tiltak ønsker Sosial- og helsedirektoratet innenfor rammene av Nasjonalt Helsenett program gjennom dette prosjektet å belyse sikkerhetsproblematikken i to kommuner med ulik størrelse og infrastruktur og komme med konkrete forslag/tiltak på området, og prøve disse ut i praksis.

Tre aktører og helsenett.

Utvexling av informasjon i helsevesenet skjer mellom svært mange og ulike aktører.

I denne sammenheng ønskes problematikken avgrenset til tre sentrale aktører;

- Sykehuset (Spesialisthelsetjenesten),
- Legekantoret (Primærlegetjenesten)
- Pleie og omsorgstjenesten

Dette er aktører med stort behov for samhandling og det prioriteres derfor en oppkobling av kommunene mot helsenett som skal ivareta sikker kommunikasjon mellom disse tre aktørene.

Kommunen som aktør i et marked med muligheter for ulike elektroniske tjenester ved tilkobling til helsenett.

De fleste norske kommuner er overveiende små aktører (75% av norske kommuner har 5.000 eller færre innbyggere) sammenlignet med sykehus (målt i antall ansatte). Dette gjelder også i sammenheng med tilkobling til helsenett. Som små aktører opplever de ofte å ha mindre frihetsgrader enn store til å prioritere inn nødvendig investering i infrastruktur og prosjektkostnader. Dette medfører at kommunene er sterkt opptatt av

kost/nyttevurderinger også i forbindelse med IT-utvikling. (Hva oppnår vi, og til hvilken kostnad?) Dette tilsier generelt at for mange kommuner er interessen for nye tjenester først til stede når det er snakk om tjenester i full drift og med høy grad av forutsigbarhet på kostnader.

Samtidig er det et faktum at svært få kommuner i dag har erfaring med helsenett. Dette gjør det til dels vanskelig for kommunene å ta stilling til prioriteringsprosjekt når det gjelder tjenester ved tilkobling til helsenett.

Hensikt med forprosjektet.

- Prosjektet skal foreslå konkrete løsninger for tilkobling til respektive regionale helsenett i kommunene Alta og Bærum. Disse løsningene skal tilfredsstillende krav til informasjonssikkerhet og samtidig være funksjonelle og kostnadseffektive. (Med funksjonalitet menes også at kommunene skal kunne ha sikker tilgang til Internett og sikker e-post.) Løsningene skal være overførbare til andre kommuner.
- De to konkrete løsningene skal inneholde kostnadsoverslag.
- Alta kommunes organisatoriske informasjonssikkerhet skal vurderes og eventuelle tiltak foreslås. Tiltakene skal være kostnadsvurderte.
- Prosjektet skal i tillegg planlegge og foreslå et hovedprosjekt for oppkobling av disse to kommunene til helsenett.

Prosjektet

Prosjektets metode og organisering.

Metode

Forprosjektet skal utarbeide konkrete løsningsforslag for to kommuner. Det forutsettes i oppdraget at disse forslagene skal være overførbare til Norges øvrige kommuner (Ca 430). Ved å velge ut Alta og Bærum håper oppdragsgiver å favne en virkelighet som består både av små og store kommuner. Samtidig er det mulig å beskrive begge de to valgte kommunene som relativt engasjerte og langt fremme i å ta i bruk IT-løsninger generelt og i helse- og omsorgstjenesten mer spesielt. Et antall på to kommuner, og samtidig to kommuner som har så vidt mye erfaring på området som Alta og Bærum, kan begrense overførbarheten til andre norske kommuner.

Prosjektet baserer sine analyser både på skriftlig og muntlige kilder. Det er i de to kommunene samlet inn skriftlig dokumentasjon på infrastruktur og sikkerhetsstruktur. Det er parallelt foretatt intervjuer med sentrale aktører i kommunene og i respektive regionale helsenett samt Nasjonalt Senter for Telemedisin. Intervjuene er foretatt ved hjelp av videokonferanse og utført med en på forhånd utarbeidet intervjuguide. (Vedlegg D) De intervjuede har posisjoner som kommunelege, omsorgssjef, IT-sjef og IT-rådgiver/konsulent. Etter analyse av skriftlig og muntlig materiale er enkelte fulgt opp med utdypende spørsmål over telefon- eller videokonferanse. I tillegg er det i forbindelse med spørsmål om omsorgstjenestens prioritering av forskjellige tjenester ved tilkobling til helsenett sendt ut et enkelt spørreskjema til de samme personene. Spørreskjemaene ble returnert i utfylt stand fra alle.

Etter analyse av dokumentasjonen er det foretatt en beskrivelse av status i de to kommunene, problembeskrivelse og forslag til prinsipielle løsningsforslag. Disse prinsipielle løsningsforslagene er så forelagt en privat aktør i markedet (Eterra AS) og videreutviklet i samarbeid med prosjektet til konkrete løsningsforslag. Disse er så brukt til å innhente en konkret prisvurdering av løsningene for de to kommunene fra samme firma.

Løsningsforslagene er så forelagt kommunene (prosjektgruppene), oppdragsgiver og referansepersoner for mulighet til kommentarer,

tilbakemeldinger og endringer.

Organisering.

Prosjektet er et forprosjekt med Sosial- og helsedirektoratet som oppdragsgiver og Kompetansesenter for IT i Helsevesenet AS som oppdragstaker. Prosjektet er finansiert og koordinert som en del av Nasjonalt Helsenett program.

En forutsetning for Sosial- og helsedirektoratets engasjement i prosjektet er Alta og Bærum kommuners forpliktende engasjement.

Prosjektleder er Tormod Hofstad, KITH. Prosjektleder rapporterer til Inger Elisabeth Kvaase, Seniorrådgiver i Sosial- og helsedirektoratet og koordinator for program Nasjonalt Helsenett.

Prosjektdeltakere fra KITH for øvrig er Arnstein Vestad og Olaf Trygve Berglihn.

Det er i hver kommune opprettet en prosjektgruppe.

- Prosjektgruppe Alta: Arnstein Vestad, rådgiver KITH, Daniel Haga, kommunelege Alta og Enst Robert Mortensen, IT-sjef Alta.
- Prosjektgruppe Bærum: Olaf Berglihn, rådgiver KITH, Eva Benedicte Liahjell, ass. kommunelege Bærum, Gunvor Erdal, seksjonssjef hjemmetjenesten Bærum (erstattet av Ann Kristin Gosse, IT-konsulent, i mai 2002), Per Chr. Solli, IT-konsulent Bærum og Siv Opheim, sikkerhetssjef Bærum.

Det er også opprettet en gruppe av referansepersoner som benyttes som ressurspersoner ved behov. Disse er: Gunn Hilde Rotvold, NST, Sissel Sunde Tveit, Bergen kommune, Jan Tore Bosåen, Østnorsk Helsenett og Morten Amundsen, Nordnorsk Helsenett.

Eterra AS, Trondheim, ved Seniorrådgiver Terje Barø har bidratt som underleverandør med de konkrete løsningsforslagene og rådgivning på informasjonssikkerhet.

Problemstilling

I bunnen av alle vurderinger rundt konkrete løsninger ligger spørsmålet hvilke tjenestebehov som skal dekkes. Dette spørsmålet forsøkes besvart innledningsvis. Videre må en finne en mest mulig effektiv og samtidig sikrest mulig tilkoblingsmåte til helsenettet. Kapitlet avsluttes med en del avgrensninger og forutsetninger som er nødvendig for å utarbeide konkrete løsningsforslag.

Hvilke tjenestebehov skal dekkes?

Når en skal foreslå en konkret måte å koble en kommunes helse og omsorgstjenester til helsenett, så er det vesentlig å definere hvilket(e) behov som skal dekkes. Avhengig av svaret kan de foreslåtte løsninger være på en skala fra ”enkle” til ”kompliserte”, og dette betinger i stor grad hvor dyre eller billige løsningene blir. Med enkel menes i denne sammenheng et behov for tjenester som fremstår som enveis kommunikasjon med tekst i form av meldinger, standardiserte eller fri tekst. Eksempler på slike tjenester er e-post og epikrisemeldingen. I den andre enden av skalaen har en tjenester som forutsetter kommunikasjon mellom to eller flere aktører samtidig, for eksempel bookingsystemer hvor en umiddelbart får svar på tidspunkt for behandling eller lignende. Likeledes krever kommunikasjon med lyd og/eller bilde mer kompliserte og omfattende løsninger.

Tilgang til både helse og sosialsystemer (herunder sensitive personopplysninger) og administrative systemer.

For en del ansatte innen pleie og omsorgstjenesten vil dette være svært aktuelt. For å ivareta begge behov vil det medføre at en får økt grad av kompleksitet i løsningene. Vi vil i avgrensning av problemstillingen definere en prioritetsrekkefølge på tilgang til tjenester som legger forutsetninger i denne sammenhengen.

Framtidig utvikling

Internett er i rivende utvikling. Til nå har fokuset for brukere særlig vært på tilgang til websider, f.eks. med nyhetstjenester, diskusjonsfora, faglige informasjonsressurser osv., samt bruk av e-post for kommunikasjon.

Dette er tjenester som i nettverkssammenheng har hatt et relativt oversiktlig spektrum av sikkerhetsmessige trusler og utfordringer som igjen har gitt opphav til et begrenset sett med sikringstiltak og verktøy for å redusere risikoen som det å åpne for kommunikasjon alltid vil føre med seg (f.eks. brannmurer, viruskontroll osv.)

Spådommer om framtiden vil alltid være usikre, men det er mulig å spore visse trender som kan gi en pekepinn på hvordan utviklingen med stor sannsynlighet vil gå. For nettverkssikkerhet vil en av disse trendene være økt kompleksitet i den nettverkstrafikken som sikkerhetsbarrierer på nettverksnivå tar sikte på å regulere. Et moteord i senere tid er "web-services" som betegner web-tilgjengelige tjenester som kan benyttes som komponenter i andre løsninger. "Web-services" beskrives som selvbeskrivende, modulære applikasjoner som kan publiseres, lokaliseres og kalles opp over nettet. Tjenestene utfører funksjoner som kan være alt fra enkle forespørsler til komplekse business-prosesser. Når en slik tjeneste er publisert kan andre applikasjoner (og andre web-services) oppdage og benytte seg av tjenesten.

"Web-services" og lignende teknologier skaper nye utfordringer for styring og kontroll av IT-løsningene. For sikkerhetsbarrierer vil det være vanskelig å skille mellom legitim og ikke-legitim trafikk. Mens disse før baserte sin policy på IP-adresser og portnummer, må de eventuelt videreutvikles til å forstå mer av den trafikken som passerer gjennom sikkerhetsbarrieren, noe som også får konsekvens for ytelsen.

Økt konvergens av IT-systemer og telekommunikasjon medfører på samme vis økt kompleksitet og nye krav til nettverkløsningene, bla. til ytelse, båndbredde og lav forsinkelse. Protokollene som benyttes for IP-telefoni og videokonferanser over IP-nett har vist seg vanskelig å sikre og har krevd spesialtilpasninger for å fungere på en tilfredsstillende måte gjennom brannmurer. Fra flere hold advares det om at innføring av telesentraler for IP-telefoni kan skape tunneler inn i virksomhetens interne nettverk. Dette kan f.eks. skje ved at gatewayer som forbinder det tradisjonelle telefonnettverket med bedriftens IP-nett angripes, eller ved svakheter i telefoniapplikasjonene som kan misbrukes.

Dette er eksempler på nye typer tjenester som man antar i større og større grad vil gjøre det vanskelig å finne og definere enkle modeller for nettverkssikkerhet som ivaretar brukergruppens behov for funksjonalitet samtidig som sikkerhetsbehovene skal ivaretas. En slik utvikling vil bla. gjøre det vanskelig å opprettholde rigide sonestrukturer basert på inndeling på nettverksnivå og stille store krav til oppfølging av sikkerhetsspørsmål både for leverandører av nettverkstjenester og som brukere av disse tjenestene.

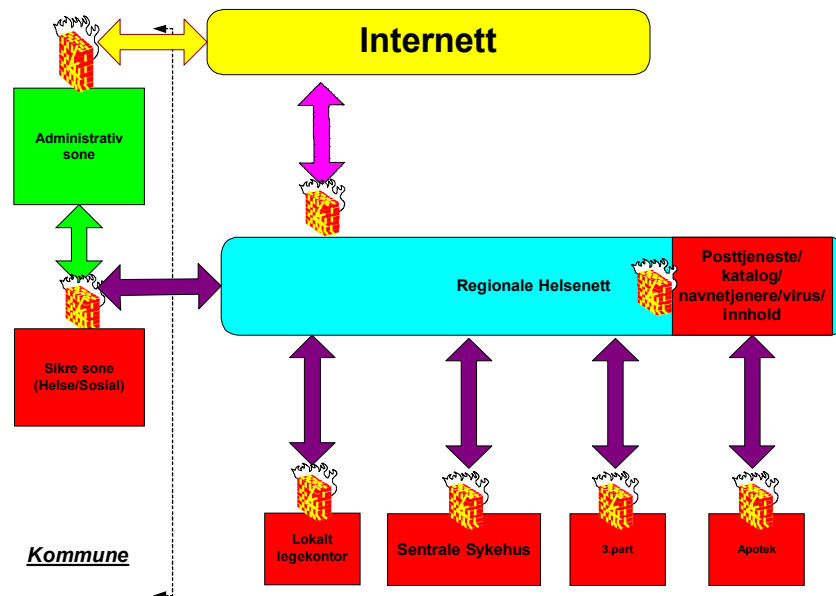
Kommunikasjon til de regionale helsenett

Følgende alternativer er skissert:

1. Tilkobling fra kommunen til regionale helsenett direkte
2. Tilkobling fra kommunen til regionale helsenett med Internett som bæretjeneste

1. Tilkobling til regionale helsenett direkte

Følgende skisse er lagt til grunn:



Her har man en direkte tilkobling til helsenett via den indre sikkerhetsbarrieren, der man har definert det regionale helsenett som en intern sone (Ref til veiledninger fra Datatilsynet).

Kommunikasjon og aksess blir styrt via den indre sikkerhetsbarrieren og aksessrouter til helsenett.

I tillegg er det opprettet en del felles tjenester i de regionale helsenett som ivaretar sikker e-post/katalogtjenester/navnetjenester etc., for eksempel ved bruk av terminalserverløsninger.

Fordeler ved bruk av direkte tilkobling til helsenett

- Man kan definere helsenettet som en del av den intern sone for kommunen
- Enklere tilkobling opp mot de tjenester som er tilgjengelig via

helsenett

- Oppsett og konfigurering av VPN inkl. kryptering er enklere
- Begrenset eksponering opp mot ”ukjent” nettverk.. Tilkoblinger til helsenett via aksesslister i routere og VPN terminatorer
- Man kan åpne for at helsenett tilbyr sikker e-post tjeneste mellom kommunene og helsenett
- Større fleksibilitet mht til å skreddersy egen tjenester og funksjoner rundt området Helse- og omsorgstjenesten

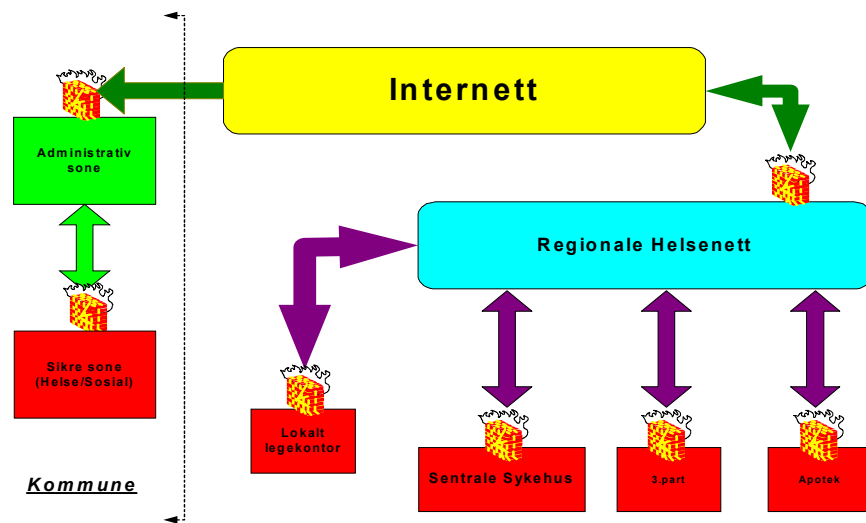
Ulemper ved bruk av direkte tilkobling til helsenett

- Flere tilknytninger til eksterne nettverk/tjenester (Internett, helsenett, 3.part etc) fra kommunene, noe som øker trusselen
- Sterkere krav til kontroll av sikkerhetsbarrierer opp mot sikker sone ved kommunene. Denne må utstyres med flere porter (fysisk Ethernet tilkobling)
- Høye kostnadene i forbindelse med etablering av linjer opp mot helsenett
- Mangel på kontroll i eget nettverk ved å sette bort tjenester (e-post, EDI, etc)

Forutsetninger for bruk av direkte kobling til helsenett

- Fast eller oppringt samband til helsenett
- Sikkerhetsbarriere av anerkjent produkt inkl. vedlikehold og oppfølging mellom sikre og intern sone hos kommunene
- En ekstra port på indre sikkerhetsbarriere som ivaretar Ethernet tilkoblingen til VPN terminator og router helsenett
- Bruk av terminalserver for lettere drift og vedlikehold av de tjenester som blir tilbudt i helsenett, herunder kryptering av informasjon for de lokasjoner som ikke har egen postserver.
- Krav til sikring av personopplysninger iht Lov om behandling av Personopplysninger (personopplysningsloven) er ivaretatt.

2. Tilkobling til helsenett med Internett som bæretjeneste



Her har man skissert en løsning der man har tilkobling til helsenett via Internett. Kommunikasjon og aksess blir styrt via den ytre sikkerhetsbarriere ved kommunen.

Fordeler ved bruk av Internett som transportvei til helsenettet

Det er i kommunens interesse å ha en tilkobling til eksterne nett og tjenester. Dette er realiserbart ved bruk av Internett.

- En tilkobling til eksterne nettverk
- En felles innfallsport til kommunen
- Sikkerheten blir ivarettatt via en egen sikkerhetsbarriere med egne soner for innhold/virus sjekking (DMZ-sone)
- E-post tilgang/web-tilgang
- Pris for tilkoblingen er billigere en tradisjonelle samband (en til en samband med flere leverandører)
- Flexibilitet mht til aksess fra flere 3. parts leverandører (f. eks IBM, Ephorma etc)

Ulemper ved bruk av Internett som transportvei til helsenettet

Internett er en bæretjeneste som er tilgjengelig for alle. Det er opp til sender og mottaker å bli enige om måter å ivareta sikkerheten på.

Det er i dag ingen garantert responstid (Noen tilbydere har kommet på

markedet)

- Mindre sikkerhet, man eksponerer seg for alle
- Kontroll av sikkerhetsbarrierer og antivirussystemer krever kompetanse
- Bruk av sikringsalgoritmer ved overføring av sensitiv informasjon (VPN, Appl. kryptering etc) krever økt kapasitet mht til maskinvare.
- Konfigurasjon av sikkerhetsbarrierer og VPN terminatorer er komplekst, da man må ha en offentlige IP-adresse på indre sikkerhetsbarriere eller VPN terminator.
- Større sjanse for at man blir utsatt for hacking
- Ikke alle 3.partsleverandører kan tilby sine tjenester pr. Internett i dag

Forutsetninger for bruk av Internett som bæretjeneste

Følgende forutsetninger er gjort ved bruk av Internett som bæretjeneste:

- Fast forbindelse til en ISP (oppringte systemer er for ustabil)
- Sikkerhetsbarriere av anerkjent merke/leverandør inkl. vedlikehold og oppfølging
- Egen DMZ-sone for kontroll av virus/http/url etc. Her bør det være automatisk oppdatering/oppgradering av antivirussystemene
- Tilknytningsnode/router av anerkjent merke
- Muligheter for å sende/transportere VPN kanaler inn mot helsenett via Internett
- Offentlige IP-adresser tilgjengelig for terminering av VPN tunneler på indre sikkerhetsbarrierer evt. VPN terminator.
- Helsenett har tilkobling/aksess til Internett
- Krav til sikring av personopplysninger iht Lov om behandling av Personopplysninger (personopplysningsloven) er ivaretatt.

Avgrensninger

Tjenestebehov

På bakgrunn av innkomne svar fra Alta og Bærum (intervju og spørreskjema) defineres kommunenes pleie- og omsorgstjenestes tjenestebehov ved tilkobling til helsenett i prioritert rekkefølge å være

som følger:

- *Sikker e-post*
- *Standardiserte meldinger*
- *Tilgang til helsenett/Internett for helserelatert informasjon (for helsearbeidere)*
- *Tilgang til intranett/intern sone/administrative systemer (for administrativt personell)*

Legekontorer som egen virksomhet og tilkobling til helsenett

Legekantorene og deres kommunikasjonsløsninger opp mot helsenett har ikke fokus i dette prosjektet. Imidlertid er legekantorene en viktig kommunikasjonspart for omsorgstjenesten, og det er slik nødvendig å definere deres forhold til kommunens øvrige løsninger for kommunikasjon mot helsenettet. I praksis må legekantorene velge mellom å defineres som en del av kommunens løsninger eller å stå som selvstendig virksomhet med eget selvstendig forhold til helsenettet. I dette prosjektet forutsettes legekantorene å ha egen tilkobling til helsenettet uavhengig av løsninger for kommunens omsorgstjeneste.

Legekantor opererer som selvstendige enheter, som oftest som private aktører, og har derfor et selvstendig ansvar for å følge kravene til informasjonssikkerhet som definert i Personopplysningsloven og tilhørende forskrift.

Forutsetninger for behandling av personopplysninger

Datatilsynet har satt ned retningslinjer med underlag i Personopplysningsloven (POL) og Forskrifter til personopplysningsloven (POF) jan/2001”

Kommuner og fylker blir i disse retningslinjene pålagt å kartlegge rutiner rundt "behandling av sensitiv informasjon".

Man har i dette forprosjektet tatt høyde for at de respektive kommuner (Alta og Bærum) har en klar strategi/policy for behandling av personopplysninger iht til POL og POF.

Følgende sikkerhetsbehov er lagt til grunn:

- *Konfidensialitet, slik at opplysninger ikke blir gjort tilgjengelig for uvedkommende*
- *Tilgjengelighet, slik at autoriserte personer med tjenestelig behov kan gjøre endringer, oppdatering, utføre vedlikehold på en tilfredsstillende måte.*

- ***Integritet, slik at opplysningene ikke utilsiktet eller uautorisert endres ved behandling eller drift.***

De(n) foreslåtte løsning(er) er basert på de retningslinjer og veiledninger som er utarbeidet av Datatilsynet for behandling av personopplysninger og Forskrifter til personopplysningsloven.

Forutsetninger for teknisk løsning

Det opprettes en tilkobling fra den indre sikkerhetsbarrieren hos kommunene inn til det regionale helsenett.

Det installeres en VPN terminator ved hver kommune for kryptering/dekryptering av data til og fra det regionale helsenett.

Det installeres en sentral VPN terminator i det regionale helsenett for kryptering/dekryptering av data til og fra kommunene. Denne sette på et eget bein (Ethernet port) på sikkerhetsbarrieren ved driftsenteret for det regionale helsenett.

For de kommuner som har egne postservere, etableres det en kommunikasjon til SMTP relè i det regionale helsenett.

For de kommuner som ikke har egne postservere, vil man etablere en sikker e-post tjeneste ved de regionale helsenett basert på terminalserver konseptet med kryptering av trafikken (ICA klient inkl. kryptering)

Navnetjeneste blir håndtert i det nasjonale helsenett.

Helsetjenesteeenhetsregisteret (HER) er også en tjeneste i nasjonalt helsenett, men kommunen er ansvarlig for at egne data er korrekte og blir oppdatert.

IP-struktur/design og oppsett av tjenester ved de regionale helsenett er gjennomført.

Domenestrukturen er avklart i de regionale helsenett.

Anbefalinger

Det anbefales at man søker å benytte en løsning der man har et minimum av tilkoblinger/ innfallsporter inn til kommunene. Internett bør være den primære innfallsporten til kommunene.

Det opprettes en egen forbindelse direkte¹ til de regionale helsenett via den indre sikkerhetsbarriere basert på bruk av terminalserverløsninger mht til sikkerhet/drift og vedlikehold. Det benyttes VPN forbindelser for utveksling av informasjon mellom de lokale posttjenerne i de ulike kommuners sikre soner. Dette gjelder de kommuner som har egne posttjenere på sikker sone.

¹ (Løsningsalternativ 1., se side 8. Denne benyttes i det videre arbeidet.)

Det benyttes en terminalbasert posttjeneste (lokalisert ved det regionale helsenett) for de lokasjoner som ikke har egen postserver på sikker sone. Her benytte en klient programvare med kryptering.

Overordnet løsning

Løsningsbeskrivelse

Kommunene er underlagt Forvaltingsloven, samt en del særlover (hjemler) som beskriver de behandlingsansvarlige og databehandlers oppgaver og rettigheter mht til bruk av elektroniske hjelpemidler (EDB-systemer).

Personopplysningsloven av des. 2001 (POL), Lov om behandling av personopplysninger og dets forskrifter, Forskrift til personopplysningsloven, (POF) beskriver de retningslinjer som er satt for behandling av personopplysninger. Dette gjelder også behandling av sensitive personopplysninger.

Kommunenes tilkobling til de regionale helsenett har som formål :

- Utveksling av informasjon mellom ulike etater/institusjoner i helsenettet
- Tilgang til informasjonssystemer

Ut i fra disse formål er det lagt vekt på følgende punkter i utforming av løsningen(e):

- 1) Informasjonssikkerhet
- 2) Fleksibilitet
- 3) Brukervennlighet
- 4) Drift/vedlikehold/rutiner

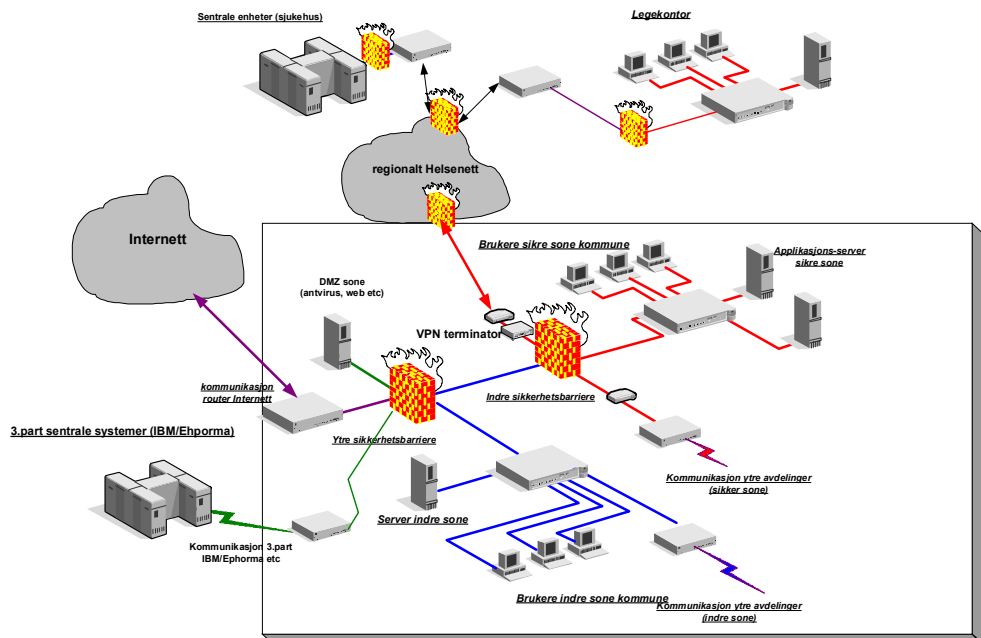
Ved elektronisk behandling av personopplysninger skal opplysningene sikres tilstrekkelig.

Det å ivareta informasjonssikkerheten er en kontinuerlig prosess, og må kontinuerlig etterprøves og forbedres. De ansatte som tar del i de systemene som inneholder personopplysninger sett i lys av personopplysningsloven, skal ha tilstrekkelig opplæring og kompetanse for drift og vedlikehold av disse systemene.

Hver etat/institusjon er selv ansvarlig for å sikre sine nettverk. Dette er

angitt med sikkerhetsbarrierer i skissen. Informasjonssikkerhet må vurderes i hvert enkelt tilfelle der brukere fra sikre soner får tilgang til Internett.

Her er angitt en generell prinsippskisse av tilkoblinger til det regionale helsenettet. I tillegg har man delt inn det lokale nettverket i to soner, definert som intern og sikker sone. Disse blir atskilt og kontrollert via sikkerhetsbarrierer.



Tilkoblinger av legekantorene er gjort med direkte tilkobling til det regionale helsenett. Kommunikasjon til sykehusene skjer via det regionale helsenett. Utsveksling av informasjon vil skje via krypterte kanaler. I tillegg vil man se på løsninger ved bruk av Terminalserver/VPN/VLAN konseptet, opp mot sentrale systemer for å differensiere sensitiv data fra kommunens øvrige data. Dette gjelder i hovedsak etater og institusjoner som skal innhente info fra sentrale systemer til sikker sone.

Som utgangspunkt har man valgt ut Alta og Bærum kommune, der man nærmere på deres behov for kommunikasjon opp mot det regionale helsenett. Løsningene for disse to kommunene er omtalt under løsningsbeskrivelse.

Punktvis oppsummering av overordnet løsning

- 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.

Alta kommune

Beskrivelse eksisterende nettstruktur.

Alta kommunes nettstruktur er basert på et stamnett av fiberlinje med 100Mbps kapasitet som knytter de ulike geografiske lokasjonene i kommunen sammen. På de ulike lokasjonene benyttes det en blanding av 10Mbps og 100Mbps Ethernet for LAN. Lokasjonene er spredt rundt i Alta kommune, med hovedtyngden i tilknytning til kommunesenteret. Pleie- og omsorgsenhetene er i hovedsak plassert på Alta Helsesenter i kommunesenteret hvor også kommunens primærhelsetjeneste holder til.

Tilkobling til eksterne nett/dataoverføring

Følgende tilkoblinger til eksterne nett finnes:

I intern sone:

- Tilkobling til Internett over 256kb linje
- Tilkobling til IBM over Frame Relay (RGAB, Folkeregister, NLP, Skatt, Komfakt, Masterpiece)
- Tilkobling til DNB over ISDN

I tillegg benyttes ISDN for å knytte mindre enheter opp mot det sentrale kommunale nettverket. Brukere i sikker sone benytter ikke disse tilkoblingene og har ikke tilgang til dem.

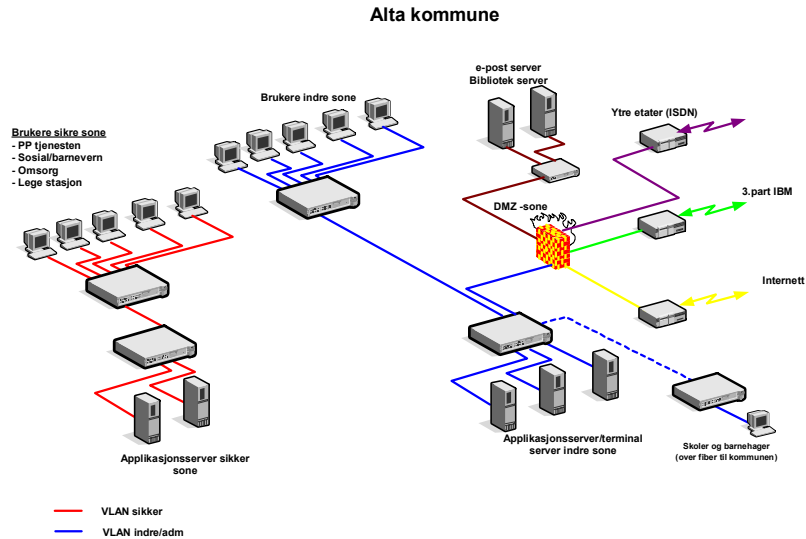
I sikker sone:

- Labsvar, sendes og mottas på legekontoets filserver med analog modem-forbindelse på 156K med 2 sykehus 1 gang pr. dag. Svarene importeres til WinMed manuelt.
- 2 MB forbindelse fra legekontoet til Helse Finnmark som benyttes til videokonferanser og i dialyseprosjektet.

Kommunikasjon med systemer i intern sone

Per i dag kommuniserer brukere i sikker sone ikke med systemer plassert i intern sone.

Følgende skisse er lagt til grunn for dagens løsning:



Oversikt over personopplysninger som behandles i kommunen

Kommunen må ha en oversikt over de personopplysninger som behandles. Denne oversikten er nødvendig bakgrunn for risikoanalyser og vil også være avgjørende for virksomhetens sikkerhetsmål og strategi. For pleie- og omsorgssektoren og primærhelsetjenesten er det særlig disse systemene som benyttes:

Informasjon, Formål	Hjemmel	Klassifikasjon	Sikringstiltak	Lagring og kommunikasjon	Registeromfang
Helseopplysninger, pasientjournal	Helseregisterloven	Sensitiv	Sikret sone	Winmed journalprogram	Ca. 35000 journaler
Helseopplysninger, pleiejournal	Helseregisterloven	Sensitiv	Sikret sone	Ephorma Profil	

I tillegg kan det finnes enkelte mindre fagsystemer, også lokalisert til sikker sone.

Ønsker for kommunikasjon med systemer i intern sone

Det er i Alta identifisert et behov for kommunikasjon med systemer i

intern sone. Behovet knyttes til ansatte med ledende funksjon som avdelingssykepleiere og eventuelt andre førstelinjeledere i omsorgstjenesten, samt personale med planleggingsfunksjoner og lederfunksjoner i helsetjenesten, eksempelvis kommunelege. Dette anslås til å utgjøre ca 12 personer i dag.

De systemer som det antas en har behov for tilgang til er saksbehandlingssystem (Kontor2000), lønssystem og regnskapssystem.

Alta kommune prioriterer tilgang til systemer i intern sone lavere enn tilgang til tjenester i helsenett.

Ønsket bruk av helsenett

Gjennom Nordnorsk Helsenett ønskes det å tilby tjenester for pleie- og omsorgssektoren i kommunen samt tilkobling for primærhelsetjenesten.

Pleie- og omsorgstjenesten anser i dag meldingstjenester som sitt største behov. Dette betyr i første rekke e-post mot legetjenesten og andre samarbeidspartnere knyttet til helsenett. Også standardiserte meldinger som epikriser er ønsket, og det er slik at behovet for sikker e-post reduseres ved økning/utbredelse av standardiserte meldinger. Det er behov for å utvikle meldinger som er spesielt innrettet mot omsorgstjenestens behov. Her nevnes medikamentmelding og legevaktsnotat. Det er viktig å kommunisere mot legekontorer og apotek.

Legetjenesten prioriterer på kort sikt tilgang til meldingstjenester. Dette er henvisninger, tolkning av røntgen, samt at en ønsker at labsvar og epikriser skal kunne gå rett inn i Elektronisk Pasient Journal (EPJ) på legekantoret. En prioriterer også kommunikasjonsmulighet (e-post) mot omsorgstjenesten i egen kommune. På noe lengre sikt ønskes tilgang til databaser og generell helseinformasjon om f.eks forhold knyttet til ventelister og behandlingstilbud. Deretter ser en også behov for toveis kommunikasjon, for eksempel bookingsystemer. Alta kommune planlegger oppkobling for legekantorene til Nordnorsk Helsenett i løpet av 2002.

Prioritet av tilgang til ulike type tjenester

Etter å ha innsamlet informasjon fra brukere/behandlingsansvarlige (sikker sone) ved Alta kommune er følgende tjenester etterspurt:

- 1) Sikker e-post (der man kan legge med vedlegg)
- 2) Tilgang til ulike tjenester
- 3) Bookingsystem (opp mot sentrale sjukehus)
- 4) Tilgang til adm. tjenester i intern sone

For å tilfredsstille disse primære tjenestene er det å anbefale en løsning

der de regionale helsenett får en sentral rolle i drift/vedlikehold og formidler av tjenestene

Teknisk løsning for Alta kommune, tilkobling til det regionale helsenett.

Alta kommune har i dag ingen kommunikasjon mellom de to definerte soner internt i kommunen.

Man vurderer å benytte terminalserver konseptet for de brukere som er tilknyttet sikker sone.

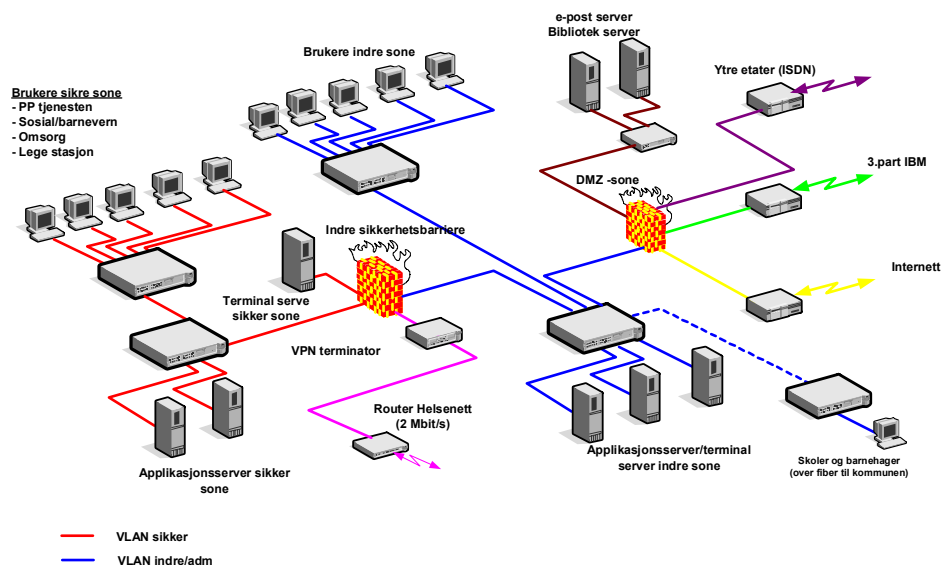
Det er i hovedsak etterspurt en del administrative tjenester fra brukere (med ledende funksjoner) i sikker sone.

I tillegg har man tatt høyde for at hovedpunktene blir oppfylt:

- 1) Informasjonssikkerhet
- 2) Fleksibilitet
- 3) Brukervennlighet
- 4) Drift/vedlikehold/rutiner

Den fysiske tilkoblingen gjøres direkte opp mot hvert regionale helsenett via en eller annen form for bæretjeneste beroende på antall brukere og tjenester som skal være tilgjengelig.

Alta kommune VLAN sikker og VLAN indre



Det blir definert to soner ved hjelp av VLAN ; intern og sikker sone som er atskilt med en sikkerhetsbarriere.

Fysisk tilkobling til det regionale helsenett er via en egen router og egen bein (Ethernet port) på den indre sikkerhetsbarrieren som vist i skissen. For opprettelse av en kryptert kanal er det installert en VPN terminator på tilkoblingen til helsenett.

Ny nettverksdesign

Med ny nettstruktur vil nettverket i hovedsak være delt i to hovedsoner, en sone for behandling av sensitive personopplysninger (sikker sone) og en sone for kommunens øvrige nett (intern sone).

Sikker sone: Den sikre sonen består av PP-tjenesten, Sosial/barnevern, Omsorg og Legestasjon. Den sensitive sonen vil i hovedsak være fysisk lokalisert til Alta Helsesenter. Her befinner servere og arbeidsstasjoner som behandler sensitive personopplysninger seg. Pr. i dag er denne sonen ikke tilknyttet kommunens øvrige nettverk. Når dette gjøres vil den sikre sonen beskyttes av en sikkerhetsbarriere i form av en brannmur.

Intern sone: Den interne sonen består av kommunens øvrige IT-nettverk og omfatter fil og printerservere, kontorstøtteprogramvare, lønnsystemer og annet, samt arbeidsstasjoner for brukere som ikke behandler sensitive personopplysninger.

Inndeling av brukere

Brukere deles inn etter den sonen de tilhører. I tillegg benyttes tilgangskontroll vha. brukernavn og passord i de applikasjonene som behandler sensitive personopplysninger. De enkelte applikasjonene har ulike typer tilgangskontroll, f.eks. benytter Ephorma Profil seg av rollebasert tilgang som sikrer at kun personell med riktig type rolle og tilknytting får tilgang til opplysninger om en pleietrengende, f.eks. kun ansatte ved en gitt avdeling.

Sikkerhetsbarrierer

Sikkerhetsbarrierer kan være både brannmurer og rutere som filtrerer nettverkstrafikken, applikasjonsproxytjenester, autentiseringsmekanismer osv.

Pr. i dag benytter Alta kommune en fullverdig brannmurløsning mellom kommunens interne nett og eksterne nett. Den sikre sonen er ikke knyttet opp mot kommunens øvrige nett og det benyttes derfor ikke brannmur for å skille ut denne sonen.

Planlagt løsning vil benytte to brannmurer, en som skiller kommunens

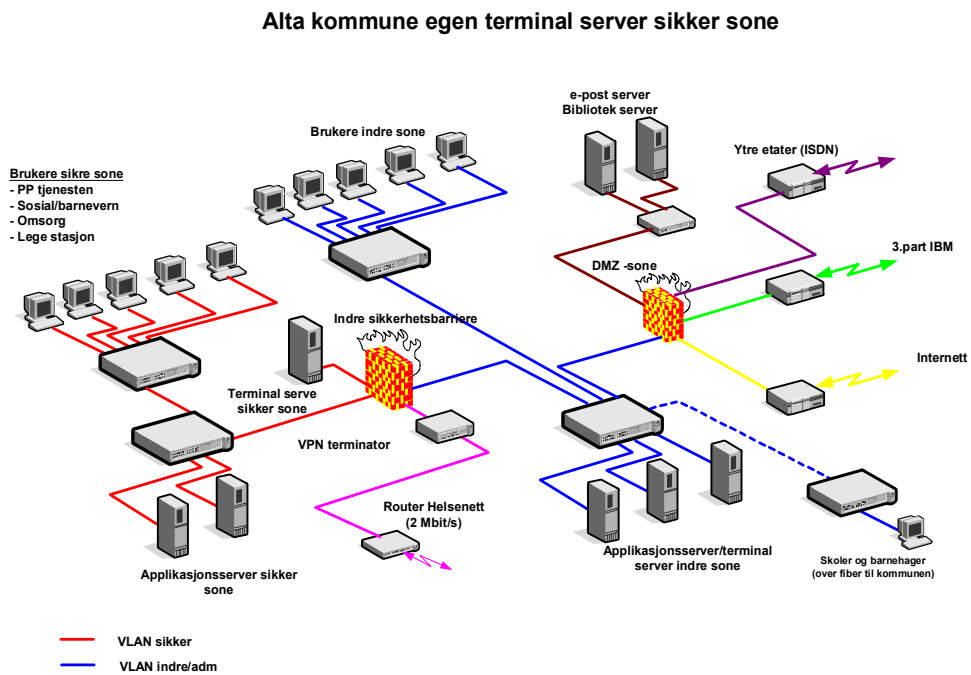
nettverk fra eksterne nett som Internett og en som skiller intern sone fra sikker sone.

Sikker e-post

Man har i realiteten to forskjellige alternative løsninger for Alta kommune:

- A. Installasjon av egen Terminal server for håndtering av e-post
- B. Ta del i en felles løsning for E-post etablert av det regionale helsenett

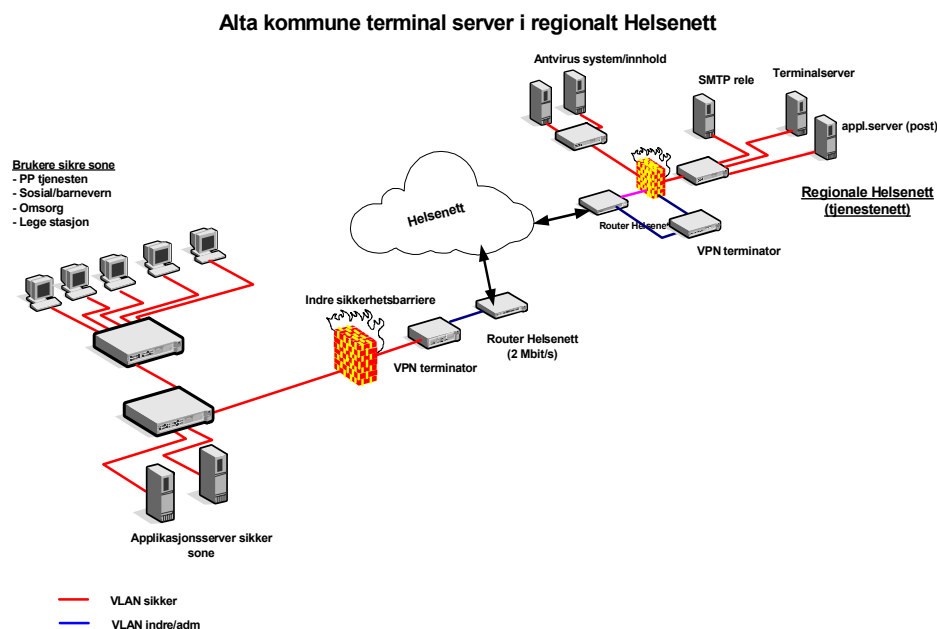
A. Installasjon av egen Terminalserver på sikker sone for håndtering av sikker e-post



Her er det installert en egen terminalserver for håndtering av sikker e-post, samt at antall lisenser er iht til tjenestene og brukerne.

For øvrig er denne løsningen lik den man har skissert for Bærum kommune.

B. Ta del i en felles løsning for E-post etablert av det regionale helsenett



Her ser man for seg en alternativ løsning der man har en terminalserver tjenesten som er opprettet i det regionale helsenett. Her vil man kunne tilby sikker e-post løsning basert på ICA-klient med kryptering opp mot de sentrale terminalserverne ved det regionale helsenett.

Det forutsettes at man har tilstrekkelige lisenser på klientene.

I tillegg har man installert en VPN terminator for kryptering av all trafikk til og fra kommunen og det regionale helsenett.

Meldingsutveksling

Det anbefales at meldingsutveksling foregår over en sentral postkasse-tjeneste, enten i det regionale helsenettet eller i nasjonalt helsenett. Sikkerhetsbarrierene må konfigureres slik at trafikk kan initieres fra dokumentasjonssystemene hos pleie/omsorg (evt. tredjeparts kommunikasjonsløsning integrert med disse) og den sentrale tjenesten,

over SMTP eller X.400 for sending og POP3/X.400 for mottak. Barrierene må konfigureres slik at nettverkstrafikk ikke skal kunne initieres fra intern sone inn mot systemene i sikker sone.

Den enkelte melding vil sikres med kryptering og eventuelt digital signatur iht. krav fra Datatilsynet og helselovgivningen for utveksling av sensitive personopplysninger.

Det benyttes VPN inkl. kryptering for sikker overføring mellom de ulike tjenester og lokasjoner.

Bookingsystem

Dette kan realiseres ved bruk av et web grensesnitt eller tilsvarende opp mot de sentrale systemer ved de respektive sykehus.

Informasjonssikkerhet kan ivaretas ved hjelp av brukernavn/passord og en kryptert VPN tunnel direkte til sykehuset, eller via den sentrale VPN terminator ved det regionale helsenett.

(Det gjøres oppmerksom på at løsninger for booking i dag oftest forutsetter at det er fastlegen (eller en annen lege) som autoriseres til å booke i spesialisthelsetjenesten systemer.)

Tilgang til administrative tjenester fra brukere på sikker sone.

Dette behovet realiseres ved bruk av en egen terminalserver på sikker sone som har forbindelse til de respektive tjenester på intern sone. Her bør man vurdere sikkerheten mht til kommunikasjon mellom den sikre og intern sone. Dette kan gjøres ved at man logger inn på to domener, eventuelt har tilgang til en egen terminalserver på intern sone. Det skal ikke være noen kommunikasjon mellom de to domene.

Tekniske spesifikasjoner Alta kommune (tilkobling) egen terminalserver.

Oppsett og konfigurasjon, samt de forutsetninger som er tatt, må belyses nærmere i Hovedprosjektet.

Indre sikkerhetsbarriere:

- Indre sikkerhetsbarriere med 4 porter (Ethernet) SW lisenser for antall IP-adresser som skal skjules.

VPN terminator:

- Egen VPN terminator inkl. 128 bits kryptering

Kommunikasjonsnode:

- Router med porter for den bæretjeneste som skal benyttes
- Kommunikasjonslinjer opp til node på det regionalt helsenett

Oppsett og konfigurering av de respektive enheter kommer i tillegg.

- Konfigurering og oppsett av sikkerhetsbarrierer
- Konfigurering og oppsett av VPN terminator
- Oppsett av router for kommunikasjon
- Tilpassing av SMTP trafikk opp mot regionale helsenett
- IP-struktur/design/domene
- Navnestandarder og tjenester
- Informasjonssikkerhet/endringsbilag

Det forutsettes at man har kommunikasjonsnode/tjenesten på plass ved det regionale helsenett.

- Sikkerhetsbarriere med min 4 port (Ethernet)
- VPN terminator for kryptering/dekryptering av data fra de ulike kommuner/legekontorer.
- Oppsett av en SMTP relè/innholdskontroll/antivirus system
- Konfigurering av VPN terminator og oppsett av sikkerhetsbarriere

Tekniske spesifikasjoner Alta kommune (tilkobling) for bruk av tjenester ved det regionale helsenett.

Oppsett og konfigurasjon, samt de forutsetninger som er tatt, må belyses nærmere i Hovedprosjektet.

Indre sikkerhetsbarriere:

- Indre sikkerhetsbarriere med 4 porter (Ethernet) SW lisenser for antall IP-adresser som skal skjules.

VPN terminator:

- Egen VPN terminator inkl. 128 bits kryptering

Kommunikasjonsnode:

- Router med porter for den bæretjeneste som skal

benyttes

- Kommunikasjonslinjer opp til node på det regionalt helsenett

Oppsett og konfigurering av de respektive enheter kommer i tillegg.

- Konfigurering og oppsett av sikkerhetsbarrierer
- Konfigurering og oppsett av VPN terminator
- Oppsett av router for kommunikasjon
- IP-struktur/design/domene
- Navnestandarder og tjenester
- Informasjonssikkerhet/endringsbilag

Det forutsettes at man har kommunikasjonsnode/tjenesten på plass ved det regionale helsenett.

- Sikkerhetsbarriere med min 4 port (Ethernet)
- VPN terminator for kryptering/dekryptering av data fra de ulike kommuner/legekontorer.
- Oppsett av en SMTP relè/innholdskontroll/antivirus system
- Konfigurering av VPN terminator og oppsett av sikkerhetsbarriere

Kostnadsoverslag

Forutsetninger:

- Terminalserver løsning for sikker sone er etablert mht til posttjeneste
- Lisenser mht til klienter er i tråd med bestemmelsene og antall brukere
- Applikasjonsserver (posttjeneste) er etablert i sikker sone inkl. SMTP protokoll
- IP struktur/domene er på plass for den sikre sonen
- Aksessrouter ved det regionale helsenett for tilkobling av kommuner og andre institusjoner. Tilhørende bæretjeneste.

Enheter/tekst	Pris veil (eks mva)	Merknader
Indre sikkerhetsbarriere	85.000,-	Checkpoint FW-1 (50) Inkl. hardware

VPN Terminator	6.000,-	Cisco 3002
Router til helsenett	6.500,-	Cisco 805

I tillegg kommer linjeleie/etablering opp mot det regionale helsenett.
(Avhengig av distanse og kapasitet)

Oppsett og installasjon kommer i tillegg.

Bærum kommune

Beskrivelse av eksisterende nettstruktur

Bærum kommune står foran en større omlegging av nettverkstrukturen. Dette er en prosess som vil gå over flere trinn hvor de er i gang med implementeringen av første trinn. Endelig kravspesifikasjon og anbudsdokumenter for andre trinn ferdigstilles høsten 2002.

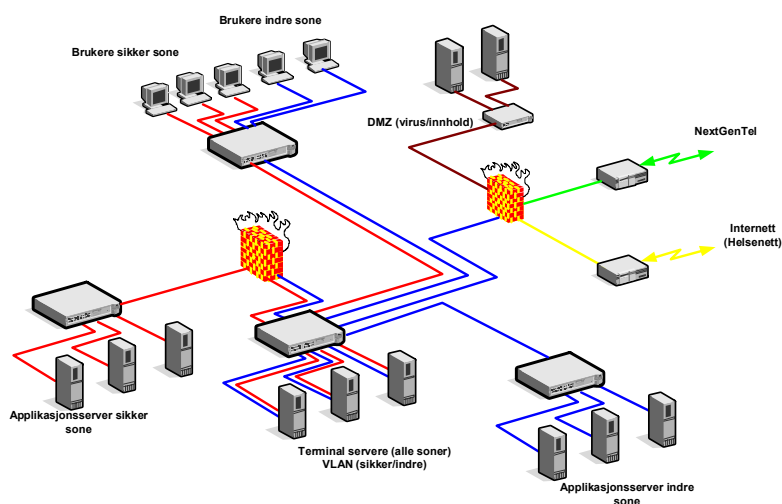
I dag benyttes prinsippet med to soner – intern og sikker sone. Arbeidsstasjoner plassert på nettverk i sikker sone har svært begrensede eller ingen muligheter for å kommunisere ut av sonen. Bærum kommune har til hensikt å plassere alle arbeidsstasjoner i eller oppkoblet mot intern sone med tilgang til applikasjoner via terminalserver plassert i egen DMZ. En del applikasjoner må oppgraderes eller skiftes ut for at de fleste brukerprogrammer skal være tilgjengelige gjennom tilkobling til terminaltjenere. Systemene som behandler personsensitive data kommer til å bli skilt ut i eget VLAN.

All tilgang til sensitiv informasjon gjøres gjennom pålogging til terminalservere på DMZ til sikker sone. Brukere som skal ha tilgang til sikker sone har to kontoer med separat pålogging: en til intern sone, og en til sikker sone. Autentiseringen styres gjennom bruk av katalogtjeneste (Netware Directory Services – NDS/E-directory). I tillegg benyttes det autentisering i applikasjonene.

Bærum kommune installerer en løsning basert på terminalserver WTS (Windows Terminal Server) løsning for intern og sikker sone.

Følgende skisse er lagt til grunn for dagens løsning:

Overordnet skisse Bærum kommune



Den interne løsningen er basert på at man benytter VLAN teknologi, der man har definert opp fire ulike VLAN:

VLAN Management, VLAN Sikker, VLAN Skole og VLAN Indre.

I tillegg er det benyttet et cluster system for kommunikasjon til andre avdelinger der man benytter høyhastighetskommunikasjon fra NextGenTel. (NGT) som også dekker tilkobling til Internett.

Oversikt over personopplysninger som behandles

I tabell 1

er det gitt en oversikt over systemer som behandler personopplysninger i Bærum kommune.

Informasjon, formål	Hjemmel	Klassifikasjon	Sikrings-tiltak	Registerets omfang
Saksbehandlingssystem for pleie og rehab. og omsorgstjenestene - modul for utlån av hjelpemidler - modul for eldresentre	Lov om helsetjenester, lov om sosialtjenester. Konesjon til føring av personregisterloven. Konesjon til føring av personregister for helse og sosialtjenesten i delt edbssystem	Personregister, sensitive data	Sikret sone	7.000-8.000 journaler
Arkivsystem	Arkivloven med forskrifter av 11. desember 1998.	Både sensitive og ikke-sensitive data.	Sikret sone. Passord og gradering per arkiv.	All inngående og utgående post.
Fraværssystem	Folketrygdeloven §25.1 og arbeidsmiljøloven §20	Personopplysninger, sensitive data	Sikret sone, passordbeskyttet	Ca. 16.000 – 18.000 personer.
Barnevernssystem Register for barnevernvakt	Lov om barneverntjenester, egen konsesjon.	Personopplysninger, sensitive data.	Sikret sone, passordbeskyttet.	ca. 800 personer.
Systemer for pedagogisk psykologiske tjenester	Opplæringsloven, egen konsesjon.	Personopplysninger, sensitive data, passordbeskyttet.	Sikret sone, passordbeskyttet	ca. 3000 personer
Konfliktråd	Lov om megling i konfliktråd, egen konsesjon	Personopplysninger, sensitive data	Sikret sone, passordbeskyttet	ca. 1700 personer.
Avlastning - funksjonshemmede	Lov om sosiale tjenester, egen konsesjon.	Personopplysninger, sensitive data.	Sikret sone, passordbeskyttet.	ca. 293 personer.
Helserapportering - helsestasjon	Lov om helsetjeneste i kommunen §1-3, A	Personopplysninger, sensitive data.	Sikret sone, passordbeskyttet.	
Sosialsystem	Lov om sosiale tjenester	Personopplysninger, sensitive data	Sikret sone, passordbeskyttet	5.500 personer.
Fritidskontakter	Lov om sosiale tjenester. Politisk vedtak mai 94.	Personopplysninger, sensitive data.	Sikret sone, passordbeskyttet	250 personer.
Klientarkiv	Lov om sosial omsorg	Personopplysninger, sensitive data	Sikret sone, passordbeskyttet	12.500 personer
Parkering	Vegtrafikkloven, forskrift om parkering for forflytningshemmede	Personopplysninger, sensitive data	Sikret sone, passordbeskyttet	1500 personer
Base - jobbtiltak	Register med informasjon om deltakere/klienter i jobbtiltak	Personopplysninger, sensitive data	Ligger på lokal server, Mølla kompetanse-senter	300 personer

Informasjon, formål	Hjemmel	Klassifikasjon	Sikrings-tiltak	Registerets omfang
Register over flyktninger og innvandrere	Lov om personregistre, egen konsesjon.	Personopplysninger, sensitive data	Sikret sone, passordbeskyttet.	
Asylsøkere - helsesystem	Helsepersonell -loven 02.07 nr. 64 1999	Personopplysninger, sensitive data	Sikret sone, passord beskyttet.	50.000
Fengsel - helsesystem	Kommunehelsetjenesteloven 19.11, nr. 66 1982	Personopplysninger, sensitive data	Sikret sone, passordbeskyttet.	900

Ønsker for kommunikasjon med systemer i intern sone

Dette er et behov som er knyttet til en ledende eller administrativ rolle, og vil bli dekket ved gjennomføring av de planer som foreligger. Dette behovet blir prioritert lavere av helse og omsorgstjenesten enn prioriterte tjenester ved tilkobling til helsenett.

Ønsket bruk av helsenett

Standardiserte meldinger og sikker e-post blir prioritert høyest, og det understrekes også i Bærum en sammenheng mellom disse to tjenestetypene i forhold til at de delvis dekker samme behov. Videre ønskes tilgang til helseinformasjon i/via nettet, mens full tilgang for alle ansatte til Internett og tjenester som krever samtidig toveis kommunikasjon ikke anses som like viktig.

Prioritet for tilgang til ulike type tjenester

Etter å ha innsamlet data fra brukere/behandlingsansvarlige (sikker sone) ved Bærum kommune er følgende tjenester etterspurt:

- 1) Sikker e-post (der man kan legge med vedlegg)
- 2) Tilgang til ulike meldingstjenester for pleie- og omsorgstjenesten
- 3) Bookingsystem (opp mot sentrale sjukehus)

Nytt nettverksdesign

Nettverket er delt i to hovedsoner, en sone for behandling av sensitive personopplysninger - sikker sone, og en sone for kommunens øvrige nett - intern sone. Sikker sone inneholder kun terminalservere (i DMZ til sikker sone) og applikasjonsservere. Ingen arbeidsstasjoner har direkte tilkobling til sikker sone.

Inndeling av brukere

Brukere autoriseres og gis tilgang til sensitive applikasjoner etter behov.

Autorisasjonen styres av stilling og kontrolleres av ansvarlig person for den aktuelle applikasjon/system – systemeieren. Tilgang sikres i flere ledd:

1. brukernavn/passord mot konto på terminaltjener
2. tilgang til applikasjoner på terminalserver styres av innslag i NDS-katalogtjener.
3. brukernavn/passord i en applikasjon, for noen systemer er tilgangsstyringen også rollebasert (Helios og moduler til denne).

Sikkerhetsbarrierer

Det benyttes brannmurklynger mellom ekstern og intern sone, og mellom intern sone og sikker sone. Tilgang til applikasjoner i sikker sone går gjennom terminaltjenere på sikker sone sin DMZ.

Tilkobling til eksterne nett

Når ny arkitektur er implementert vil kommunens lokasjoner benytte G.SHDSL-tilkobling til et fiber stamnett fra NextGenTel. Tilkobling til Internet går fra ytre brannmurklynge. Bærums sykehjem i Altea, Spania, vil være knyttet opp mot intern sone via Internet med VPN-tunnel. All tilgang til applikasjoner er gjennom terminalprogramvare med kryptert forbindelse til terminaltjenere.

Anbefalt teknisk løsning for Bærum kommune, tilkobling til det regionale helsenett.

Man har her tatt utgangspunktet i den overordnede løsningen samt den informasjon som er innsamlet i WTS prosjekt som Bærum har med Eterra.

I tillegg har man tatt høyde for at hovedpunktene blir oppfylt:

1. **Informasjonssikkerhet**
2. **Fleksibilitet**
3. **Brukervennlighet**
4. **Drift/vedlikehold/rutiner**

Generelt

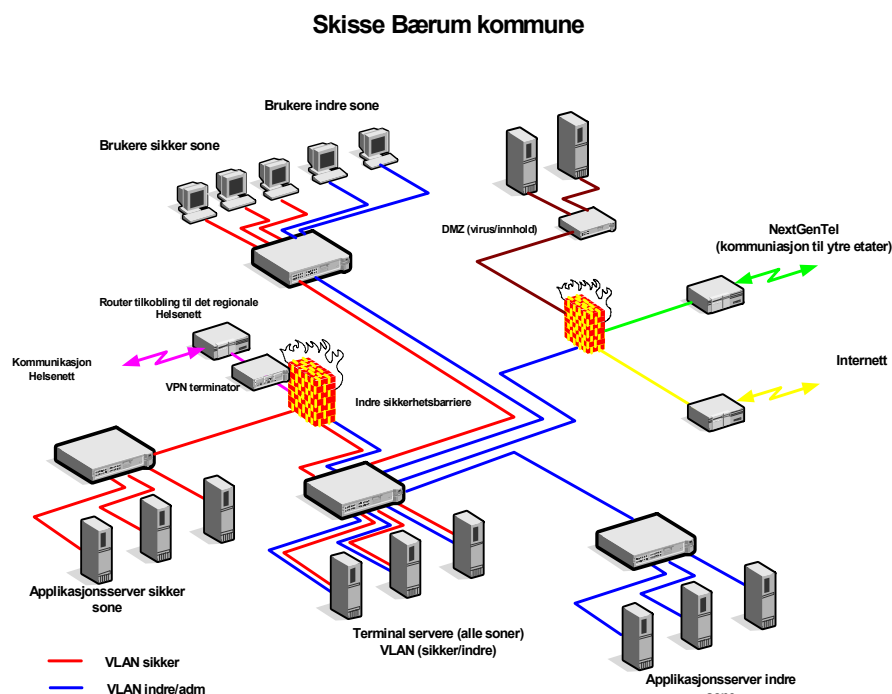
For å tilfredsstille disse primære kravene er det å anbefale en løsning der de regionale helsenett får en sentral rolle i drift/vedlikehold og formidler av disse tjenestene.

Tilkoblingen gjøres direkte opp mot regionalt helsenett via en eller annen form for bæretjeneste beroende på antall brukere og tjenester som skal

være tilgjengelig.

Bærum kommune

Tilkoblingspunktet er fra indre sikkerhetsbarriere ved kommunen som vist i følgende skisse:



Sikker e-post

Dette er definert som e-post som blir benyttet av brukere internt i sikker sone. Post kan inneholde både sensitive /ikke sensitive personopplysninger uten restriksjoner så lenge posten ikke forlater sikker sone.

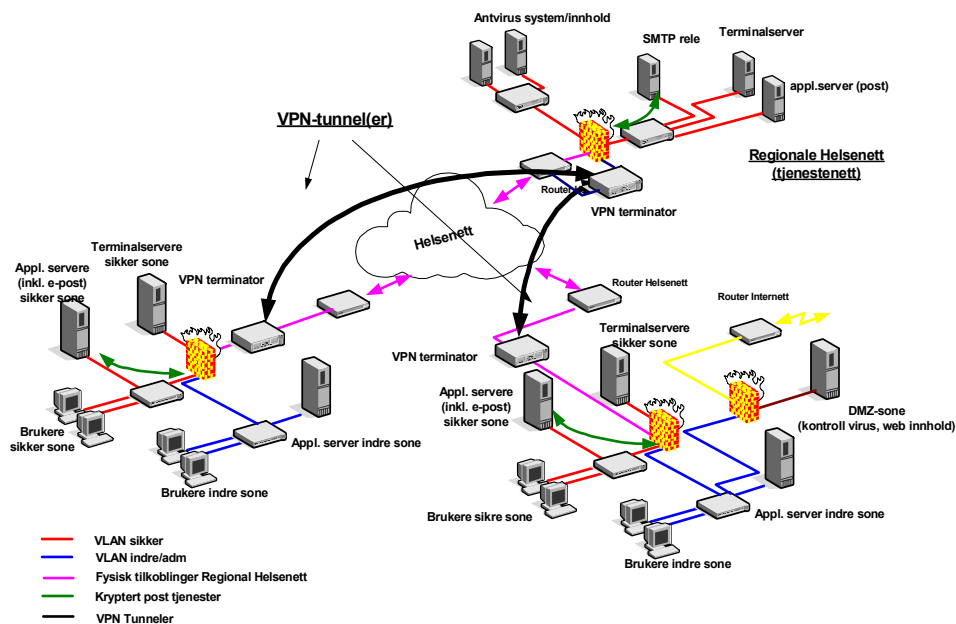
Tjenesten nås av brukere på sikker sone via terminalserver (sikker sone) og en postklient (GroupWise) opp mot en post server i sikker sone (appl. serverene sikker sone).

Det er ikke behov for kryptering av denne tjenesten ved internt bruk i sikker sone.

Sikker e-post mot ytre etater (via NextGenTel) vil bli kryptert via ICA-protokollen opp terminalserveren(e).

Sikker e-post til andre institusjoner/kommuner setter høye krav til informasjonssikkerhet ref til POL og POF. Dette løses teknisk sett ved at man setter opp egne VPN tunneler mellom de ulike institusjoner der datautvekslingen skjer via kryptert forbindelser mellom serverne. For utveking av e-post benyttes SMTP/x.400 protokollen mellom servere.

Navneoppslag/design/katalogtjenester blir ivaretatt av et eget SMTP relè i hvert regionale helsenett. Dette relè holder rede på alle postserverene som er tilknyttet helsenettverket.



Her er det skissert en forbindelse mellom to kommuner innenfor samme regionale helsenett.

En VPN tunnel blir etablert opp mot det regionale helsenettets (tjeneste nett) SMTP relè. Denne gjør oppslag opp mot mottakers post server og setter opp en VPN-tunnel mot denne lokasjonen.

Etter at VPN-tunnelene er opprettet vil data/post flyte fra den ene postserveren til den andre. Data/posten blir kryptert når den forlater sikker sone (avsender) og dekryptert når den kommer inn til sikker sone (mottaker) via egne VPN terminatorer.

Sikker E-post mellom lokasjoner som har tilhørighet i forskjellige regionale helsenett, bør styres av et overordnet nettverk som kan tilby SMTP tjenester.

På sikt vil PKI-løsninger kunne erstatte VPN. Det er imidlertid i dag få løsninger for PKI, og de er i dag også dyrere. Vi har derfor benyttet VPN

i løsningsforslaget. Når dette sannsynligvis endrer seg på sikt vil VPN kunne benyttes til kommunikasjon og oppdatering mellom serverne og PKI til kontroll og sikkerhet ved oppkobling av brukere mot sentrale systemer.

Meldingsutveksling

Det anbefales at meldingsutveksling foregår over en sentral postkasse-tjeneste, enten i det regionale helsenettet eller i nasjonalt helsenett. Sikkerhetsbarrierene må konfigureres slik at trafikk tillates mellom dokumentasjonssystemene hos pleie/omsorg (evt. tredjeparts kommunikasjonsløsning integrert med disse) og den sentrale tjenesten, over SMTP eller X.400 for sending og POP3/X.400 for mottak. Barrierene må konfigureres slik at trafikk ikke tillates inn mot systemene i sikker sone.

Den enkelte melding vil sikres med kryptering og eventuelt digital signatur iht. krav fra Datatilsynet og helselovgivningen for utveksling av sensitive personopplysninger.

Det benyttes VPN inkl. kryptering for sikker overføring mellom de ulike tjenester og lokasjoner.

Bookingsystem

Dette kan realiseres ved bruk av et web grensesnitt eller tilsvarende opp mot de sentrale systemer ved de respektive sykehus. Sikkerhet kan ivaretas via bruker/passord og en kryptert VPN tunnel direkte til sykehuset, eller via den sentrale VPN terminator ved det regionale helsenett.

Tilgang til administrative tjenester fra brukere på sikker sone.

Dette behovet realiseres ved bruk av en egen terminalserver på sikker sone som har forbindelse til de respektive tjenester på intern sone. Her bør man vurdere sikkerheten mht kommunikasjon mellom den sikre og intern sone. Dette kan gjøres ved at man logger inn på to domener evt. har tilgang til en egen terminalserver på intern sone.

Tekniske spesifikasjoner Bærum kommune, tilkobling til helsenett

Oppsett og konfigurasjon, samt de forutsetninger som er tatt, må belyses nærmere i Hovedprosjektet.

Indre sikkerhetsbarriere:

- Ethernet/port opp mot router for kommunikasjon til helsenett

VPN terminator:

- Egen VPN terminator inkl. 128 bits kryptering

Kommunikasjonsnode:

- Router med interface for den bæretjeneste som skal benyttes opp mot helsenett
- Kommunikasjonslinjer opp til node i det regionale helsenett

Oppsett og konfigurering av de respektive enheter kommer i tillegg.

- Konfigurering av sikkerhetsbarrierer
- Oppsett av router for kommunikasjon
- Oppsett av VPN terminator
- Tilpassing av SMTP trafikk opp mot Regionale helsenett
- IP-struktur/design/domene
- Navnestandarder og tjenester
- Informasjonssikkerhet/endringsbilag

Det forutsettes at man har kommunikasjonsnode/tjenesten på plass ved det regionale helsenett.

Kostnadsoverslag

Forutsetninger:

- Terminalserver løsning for sikker sone er etablert mht til posttjeneste
- Lisenser mht til klienter er i tråd med bestemmelsene og antall brukere
- Applikasjonsserver (post) er etablert i sikker sone inkl. SMTP protokoll
- Indre sikkerhetsbarrierer er etablert med de respektive nettverkskort
- IP struktur/domene er på plass for den sikre sonen
- Aksessrouter ved det regionale helsenett for tilkobling av

kommuner og andre institusjoner. Tilhørende bæretjeneste.

Enheter/tekst	Pris veil (eks mva)	Merknader
VPN Terminator	7.000,-	Cisco 3002
Router til helsenett	6.500,-	Cisco 805

I tillegg kommer linjeleie/etablering opp mot det regionale helsenett.
(Avhengig av avstand og kapasitet)

Oppsett og installasjon kommer i tillegg.

Organisering av informasjonssikkerheten i Alta kommune

Kapittel

8

Bakgrunn

I tillegg til innføringen av den tekniske løsningen må kommunen etablere en sikkerhetsorganisasjon og et styringssystem for informasjonssikkerhet. Dette kapittelet vil kort beskrive de viktigste elementene som må inngå i et slikt styringssystem. Et hovedprosjekt må forutsette at et slikt system er etablert i tråd med personopplysningsloven og tilhørende forskrift. Dette arbeidet er i henhold til prosjektdirektivet vurdert og beskrevet for Alta kommune. Bærum kommune har på sin side gjort et stort arbeid for å utarbeide dokumentasjon, håndbok og gjennomført en sikkerhetskampanje.

Lov om behandling av personopplysninger (POL)

Man tar her utgangspunktet i de ulike personopplysninger som behandles i kommunen. Disse blir kartlagt mht til grad av gradering (beskyttelsesgrad). Deretter ser man på trusselbildet ut fra følgende kriterier:

- *Konfidensialitet, slik at opplysninger ikke blir gjort tilgjengelig for uvedkommende*
- *Tilgjengelighet, slik at autoriserte personer med tjenestelig behov kan gjøre endringer, oppdatering, utføre vedlikehold på en tilfredsstillende måte.*
- *Integritet, slik at opplysningene ikke utilsiktet eller uautorisert endres ved behandling eller drift.*

Her er angitt en tabell mht til trusselbildet og kriteriene:

For å forstå behovet for sikkerhet sett i lys av formålet for behandlingen, er det viktig å ha god oversikt over den informasjon som behandles.

Tabellen under benyttes av virksomheten for å få en oversikt over hvilken informasjon som behandles i hvilke systemer.

System	Klassifikasjon	Formell sikkerhetskrav *)
Helseopplysninger: <ul style="list-style-type: none"> • Pasientjournal • Helse opplysninger 	Sensitive Personopplysninger	POL (M)
Barnevern <ul style="list-style-type: none"> • Vurdering og tiltak • Registre over søkere • Registre for vilkår kontaktstøtte • Uttalelser i barnevernsaker 	Beskyttelsesverdige Personopplysninger	POL(M/K)
Pleie og omsorg: <ul style="list-style-type: none"> • Søknader/vurderinger/tildelinger 	Beskyttelsesverdige Personopplysninger	POL(M)
Sosial tjenester <ul style="list-style-type: none"> • Klientøkonomi • Sosiale ytelser 	Beskyttelsesverdige Personopplysninger	POL(K)
Vaksinasjonsregistre	Personopplysninger	Egen konsesjon (M/K)
Egenbetaling opphold i sykehjem	Personopplysninger	POL (I)
Bostøtte/sosialtjenesten	Personopplysninger	POL (K), sentralt
Registre for sykefravær <ul style="list-style-type: none"> • Oppfølging sykemeldte 	Beskyttelsesverdige Personopplysninger	POL(M), sentralt
Arbeid med bistand <ul style="list-style-type: none"> • arbeidssøkere • arbeidstakere 	Personopplysninger	POL(M)

Tabell: Oversikt over virksomhetens informasjon.

**) M: Meldeplikt; K: Konsesjon; I: Ingen (evt. egen)*

Avhengig av det aktuelle system og informasjonen som behandles, vil de ulike aspektene ved sikkerhet (konfidensialitet, integritet og

tilgjengelighet) ha ulik betydning. Følgende kategorisering kan knyttes til brudd på sikkerhetsbehovene:

Stor (S)

- Konfidensialitet – svært sårbare og kritiske opplysninger
- Integritet – kritiske bedrifts- og personopplysninger og økonomiske transaksjoner
- Tilgjengelighet – Eksempel: Opptil en halv time nedtid i arbeidstiden. Ved reduksjon i tilgjengeligheten vil effektivitet og den totale behandlingskapasiteten bli drastisk redusert.

Middels (M)

- Konfidensialitet – beskyttelseverdige informasjon i bruddstykker uten sammenheng (f. eks temporære filer)
- Integritet – opplysninger unntatt offentlighet samt interne virksomhetskritiske opplysninger
- Tilgjengelighet - Opptil en halv dag nedtid i arbeidstiden

Lav(L)

- Konfidensialitet – Små krav til beskyttelse, registre uten beskyttelsesverdige informasjon
- Integritet – opplysninger av intern betydning som adressekataloger, statistikk, intern e-post
- Tilgjengelighet – Eksempel: Opptil 2-3 dager nedetid

Ubetydelig (U)

- Konfidensialitet – Ingen spesielle krav til beskyttelse, offentlig informasjon
- Integritet – ubetydelige konsekvenser ved endring
- Tilgjengelighet – Eksempel: Opptil en uke nedtid

Med utgangspunkt i skalaen ovenfor, kan tabellen under gir et forslag til kategorisering av noen typiske informasjonstyper som behandles i ulike virksomheter:

Informasjon/System	Konfidensialitet	Integritet	Tilgjengelighet
Helse og sosial opplysninger	S	S	M
Barnevern	S	S	M
Pleie og omsorg	S	S	M
Journaler med sensitive opplysninger	S	S	M
Vaksinasjonsregistre	M	M	M
Egen betaling opphold sykehjem	M	M	L
Bostøtte/sosialtjenesten	M	M	U
Registre over sykefravær	S	S	M
Arbeid med bistand	M	M	L
Flyktning registre	S	S	L

Tabell Kategorisering av informasjon

Som man ser av tabellen er de registre som inneholder sensitive personopplysninger iht. til personopplysningsloven klassifisert til S på konfidensialitet og S for Integritet.

Tilgjengelighet er begrunnet med krav til oppetid og respons.

Vurderinger og anbefalinger

Det anbefales at sikkerhetsledelsen deles i to ansvarsområder:

- Operativt sikkerhetsansvar som definerer kommunens sikkerhetsmål, -strategi og -policy og har et kontrollerende og koordinerende ansvar. I større kommuner opprettes gjerne en egen funksjon/stilling med dette ansvaret. I mindre kommuner vil vi anbefale at dette ansvaret bør ligge hos rådmannen, med støtte fra kompetanse i IT-avdelingen. Siden det er ønskelig med et tydelig skille mellom operativ og utførende ansvar bør stillingsinstruks for personell med denne funksjonen klargjøre denne ansvarslinjen som uavhengig av linjeansvar til IT-sjef.
- Utførende sikkerhetsansvar bør ligge hos IT-avdelingen ved IT-sjef. Dette ansvaret innebærer bl.a. å forvalte vedtatt sikkerhetspolicy, gjennomføre risikoanalyser iht. vedtatt norm ved innføring av nye IT-løsninger eller endringer i eksisterende løsninger.

I tillegg bør den enkelte systemeier (hvis andre enn IT-avdelingen) ha et selvstendig ansvar for sikkerheten i sine systemer.

Ansvar

Det øverste ansvaret for kommunens informasjonssikkerhet ligger hos kommunens ledelse, dvs. rådmann og ordfører m. kommunestyret. Det anbefales at rådmannen gis det operative sikkerhetsansvar med støtte fra kompetanse i IT-avdelingen. Ansvaret innebærer særlig å utarbeide/godkjenne sikkerhetsmål og –strategi. I tillegg må ansvaret for risikovurderinger og avviksbehandling plasseres.

Dokumentasjon

Lovverket stiller krav til dokumentasjon av informasjonssikkerheten. Dette innebærer bla.:

- Sikkerhetsmål og strategi
- Oversikt over personopplysninger som behandles (se neste avsnitt)
- Informasjon om ansvarsforhold, evt. organisasjonskart
- Informasjon om partnere og leverandører
- Rutiner og retningslinjer

Det anbefales at en prosjektgruppe etableres med ansvar for å bygge opp den nødvendige dokumentasjonen.

Oversikt over behandling av personopplysninger

Det må etableres en oversikt over all behandling av personopplysninger som foregår i kommunen. Dette kan foregå ved at prosjektgruppen sender ut et kartleggings skjema til alle systemeiere/behandlere av personopplysninger. Dette skjemaet må inneholde felter for bl.a.:

- Systemeier
- Hvorvidt behandlingen foregår med elektroniske hjelpemidler eller manuelt
- Hvor behandlingen foregår (fysisk plassering av brukere)
- Formål med behandlingen
- Hvorvidt opplysningene som behandles er sensitive, typen personopplysning som behandles (f.eks. persondata, fødselsnummer, kjønn, rase, preferanser osv.) og evt. lovgrunnlag for behandling av sensitive opplysninger iht. POL §9.
- Hvorvidt opplysningene utleveres til andre, i så fall hvem.
- Evt. vurdering av sannsynlighet/konsekvens ved sikkerhetsbrudd

Rutiner

Kommunen må etablere et sett av rutiner for oppfølging av sikkerhetsledelsen. Særlig viktig er et system for avvikshåndtering, risikovurdering, årlig gjennomgang av sikkerheten utført av kommunens ledelse samt sikkerhetsrevisjon. I tillegg bør det utarbeides rutiner for arbeidet med informasjonssystemet, særlig konfigurering av tekniske sikkerhetsløsninger.

Avvikshåndtering

Ansvar: Den som oppdager avviket, IT-sjef, sikkerhetsansvarlig

Kommunen må ha et system for håndtering av avvik i sikkerhetsstyringen som kan sikre at avvik oppdages og rapporteres samt at nødvendige korrigerende tiltak, både kortsiktige og langsiktige vurderes og gjennomføres. Som avvik bør regnes:

- Eksponering av personopplysninger til uautoriserte, utilsiktet eller med forsett
- Uautorisert bruk av informasjonssystemene og brudd på kommunens retningslinjer for IT-sikkerhet
- Manglende tilgang til informasjonssystemene
- Feil eller konfigurasjonsfeil i IT-løsningene (særlig sikkerhetsløsningene) som har betydning for IT-sikkerheten
- Brudd på rutiner for IT-sikkerhet

Avvik bør rapporteres på eget skjema som inneholder felt for beskrivelse av avviket, tiltak som er iverksatt, informasjon om involverte parter og systemer og evt. forslag til langsiktige tiltak.

Ansvar for oppfølging av tiltak må fordeles på den enkelte linjeleder, IT-avdeling og sikkerhetsansvarlig. Avvik og tiltak bør også vurderes i ledelsens gjennomgang.

Risikovurdering

Forskrift til POL §2-4 stiller krav til at kommunen skal gjennomføre risikovurderinger for å kartlegge sannsynlighet for og konsekvens av sikkerhetsbrudd. Det bør etableres en mal og prosedyre for gjennomføring av slik vurdering, jfr. f.eks. Datatilsynets veiledning i risikoanalyse.

Ledelsens gjennomgang

Ansvar: Rådmann

Kommunens ledelse må minimum årlig utføre en gjennomgang av informasjonssikkerheten. Dette innebærer å vurdere sikkerhetsmål og strategi, vurdere hvorvidt de tiltak som er innført er egnet/tilstrekkelige til å oppnå målsetningen. Innrapporterte avvik av betydning kan tjene til

å belyse hvorvidt dette er tilfelle i tillegg til resultatet av sikkerhetsrevisjonen.

Sikkerhetsrevisjon

Ansvar: Kommunerevisjonen

Informasjonssikkerheten skal revideres jevnlig for å kontrollere at sikkerhetstiltak er formålstjenlig og effektive. Ansvar for dette kan ligge hos kommunerevisjonen, evt. kan eksterne benyttes for revisjonen. Jfr. forskrift til POL §2-5

Kostnadsoverslag

Kostnadene er avhengig av kommunens størrelse (antall ansatte, geografisk spredning og organisasjon). For Alta kommune er det innhentet en prisantydning på minimum kr. 50.000,- i tillegg til arbeidstid/arbeidsinnsats fra kommunens behandlingsansvarlige og andre interne personer som måtte delta.



Prosjektplan hovedprosjekt

Avgrensninger og forutsetninger

I prosjektdirektivet beskrives målsettingen for et hovedprosjekt som ”oppkobling av kommunal omsorgstjeneste og primærlegetjeneste i Alta og Bærum til sine regionale helsenett”.

I forprosjektet har omsorgstjenesten prioritet og er prosjektets fokus. Dette videreføres også i hovedprosjektet. I plan for hovedprosjektet forutsettes det derfor at legekantorenes tilkobling til helsenett er en utenforliggende (for hovedprosjektet) og selvstendig oppgave. Disse to selvstendige oppgavene kan imidlertid sannsynligvis ses på som gjensidige å øke hverandres nytteverdi i en kost/nytte analyse. Dette tilsier at de vurderes gjennomført i en sammenheng.

I forbindelse med etablering av forprosjektet ble det drøftet hvor langt i utviklingsprosessen et eventuelt hovedprosjekt burde gå. Med dette menes spørsmålet om hvorvidt et hovedprosjekt skulle inkludere testing av en eller flere tjenester eller ikke. En av tjenestene nevnt i forbindelse med utformingen av prosjektdirektivet for forprosjektet var standardiserte meldinger for pleie og omsorgstjenesten. Konklusjonen var at hovedprosjektet og utprøving av tjenester skulle skilles ad, og at det er opp til de involverte parter å søke etablering av anvendelsesprosjekt(er) etter at hovedprosjektet er avsluttet.

Dette medfører at hovedprosjektets målsetting er å etablere løsningene beskrevet i forprosjektet så langt at det er klart for testing av tjenester. Dette tilsier at en etter hovedprosjektets avslutning vil kunne få erfaringer med hvordan løsningene fungerer i praksis og en må være åpen for å gjøre nødvendige tilpasninger.

I hovedprosjektet vil det inngå flere selvstendige parter. Både Alta kommune, Bærum kommune, Østnorsk Helsenett og Nordnorsk helsenett vil måtte ta egne selvstendige avgjørelser om deltakelse basert på vurdering av egne interesser og muligheter. I tillegg ser en ikke at det vil være store forskjeller i effektivitet avhengig av grad av samordning mellom Alta og Bærum, da sett bort fra selve prosjektledelsen/administrasjonen som bør være felles hvis prosjektet etableres i begge kommuner. Hovedprosjektet er derfor basert på en struktur som innebærer at det gjennomføres i to relativt selvstendige og uavhengige deler. En i Alta/Nordnorsk Helsenett og en i

Bærum/Østnorsk helsenett. Også de økonomiske størrelser er beregnet med en slik struktur.

Prosjektets faseinndeling og hovedmilepæler

Med utgangspunkt i løsningsskissene for Alta og Bærum vil prosjektet ha følgende faser:

1. Etablering av prosjektet og utforming av detaljert kravspesifikasjon med definerte etableringskriterier for hver kommune.

Hovedmilepæl 1. Godkjente Kravspesifikasjoner foreligger.

2. Innhenting av tilbud eller anbud på beskrevet utstyr og arbeid.

Hovedmilepæl 2: Leverandør(er) er valgt.

3. Tilkobling til helsenett: Montering og konfigurering.

Hovedmilepæl 3: Definerte etableringskriterier nådd. Klart til testing av anvendelser/tjenester.

Dokumentasjon/erfaringsmateriale utarbeidet.

Prosjektets gjennomføringstid

Tid til gjennomføring er basert på antakelser knyttet til prosjektfasenes deloppgaver, her oppsummert pr. prosjektfase og totalt. De to samme tidsmessige forløp er forutsatt i både Alta og Bærum. (NB: Nødvendig tid til anbudsutarbeidelse fra anbydere må sjekkes med gjeldene lov/regelverk, og eventuelt tillegg innarbeides i planens fase 2.)

Fase 1: 8 uker

Fase 2: 7 – 9 uker

Fase 3: 10 uker

Samlet tidsbruk: 26 uker, eller ca 6 1/2 mnd.

Det forutsettes i planleggingen av hovedprosjektet at det foretas en beslutning om iverksettelse så tidlig at oppstartsdato blir 1. september 2002. Det vil slik kunne gjennomføres 16 av 26 uker i 2002, og 10 i 2003. I tillegg kommer en uke juleferie/nyttår. Dette tilsier avslutning av prosjektet før påske 2003. Ekstra beslutningstid kommer i tillegg. Hovedprosjektet må i fase 1 utarbeide en nøyaktig prosjektplan.

Organisering av prosjektet

Prosjektet organiseres som to uavhengige arbeidsprosesser med felles prosjektledelse.

Styring

Prosjektet knyttes til finansieringskilde/oppdragsgiver enten med direkte rapportering fra prosjektet eller til opprettet styringsgruppe. Første alternativ anbefales, men må nærmere avklares når finansiering er avtalt. Det gjennomføres styringsmøte mellom oppdragsgiver og utfører ved avslutning av fase 1 og 2 for informasjon og drøftinger av neste prosjektfase.

Felles prosjektledelse tenkes som kun en prosjektleder. Denne skal ha ansvar for prosjektetablering og nødvendig koordinering, samt utarbeiding av erfaringsdokument og annet erfarings- og formidlingsmateriale.

Arbeidsgrupper

Det etableres en liten prosjektgruppe i hver kommune bestående av representant fra kommuneledelsen, omsorgstjenesten, IT-avdeling/IT-faglig kompetanse i kommunen og representant for regionalt helsenett. Det avholdes felles oppstartsmøte for de to arbeidsgruppene. Arbeidsgruppen vurderer innkomne tilbud/anbud, men beslutning om valg av leverandør overlates Rådmannen i de to kommunene eller den disse måtte bemyndige. Når leverandør(er) er valgt er det naturlig å invitere representant derfra inn i arbeidsgruppen. Arbeidsgruppene møtes fast minimum 1 dag i måneden og deltakerne arbeider selvstendig mellom møtene.

Erfaringskonferanse/workshop

Det avholdes en workshop for å få fram erfaringer fra prosjektet med fokus på det som måtte være av interesse for andre kommuner og andre interessenter til løsningene. Resultatene benyttes som grunnlag for utarbeidelse av projektrapport/erfaringsdokument.

Økonomi generelt

Det er flere økonomiske aspekter i prosjektet. Det hefter også usikkerhet til flere sider ved den økonomiske vurderingen. Det har vært et mål for forprosjektet å presentere økonomiske vurderinger av et hovedprosjekt egnet til å ta en beslutning om prosjektetablering og til å få frem eventuelle behov for ansvarsavklaringer mellom ulike involverte aktører.

Som utgangspunkt har vi tatt at ansvar for finansiering følger av ansvar for løsninger. Slik vil det framgå et finansieringsansvar for to parter; regionalt helsenett og kommune. Vi tar utgangspunkt i de fysiske løsninger og ser på hva det er naturlig at de to partene har eierskap til

etter prosjektets avslutning. Vi har ikke avklart om det er grunnlag for å bryte en slik struktur i forbindelse med et konkret hovedprosjekt, for eksempel ved at staten finansierer større deler av, eller hele prosjektet. Dette har for eksempel vært vanlig ved pilotprosjekter i spesialisthelsetjenesten. Vi har heller ikke tatt stilling til eventuell fordeling av kostnader mellom program nasjonalt helsenett og de regionale helsenett.

Vi har i forslag til plan for hovedprosjektet lagt inn følgende forutsetninger på dette området:

- a. Løsninger for sikker e-post er et ansvar for helsenett.
- b. Nødvendige sikkerhetstiltak i kommunen som soneinndeling, terminalservere, brannmurer og lignende er et ansvar for kommunen selv.

Prosjektkostnadene består av flere typer utgifter og ressursinnsats.

- Utgifter til anskaffelse av fysisk infrastruktur som routere, servere, kabel, fysisk sikring osv
- Utgifter til montering, konfigurering og testing av fysisk infrastruktur kjøpt av leverandør(er)
- Egeninnsats fra de deltagende aktører i forbindelse med fysisk tilkobling til helsenett.
- Utgifter til ekstern prosjektledelse, prosjektadministrasjon og utarbeidelse av erfaringsmateriale.
- Egeninnsats fra de deltagende aktører i forbindelse med prosjektgjennomføring, herunder møtedeltakelse, reiseutgifter og lignende.

I tillegg kommer spørsmål om driftsutgifter etter at prosjektet er gjennomført. Dette er et moment som kan ha betydning for de beslutninger som skal taes, og som må holdes opp mot den antatte nytteverdi av å ha løsningene etablert. Det er i noen relevante sammenhenger forsøkt å antyde løpende utgifter. Disse finnes i tabellene.

Med den forutsatte prosjektlengde (26 uker) og oppstart 1. september 2002 vil prosjektets kostnader kunne tenkes periodisert med ca 604.000,- i 2002 og 377.000,- i 2003. Dette vil imidlertid kunne bli feil hvis utgiftene til utstyranskaffelser og montering/konfigurering følger en annen periodisering i det konkrete pilotprosjektet.

Alle priser oppgitt er veiledende priser eksklusive MVA.

Konkrete kostnadsanslag

Det er her tatt inn utgifter og ressursinnsats vedrørende nødvendige utstyranskaffelser og tilsvarende arbeidsinnsats som montering og konfigurering. Utstyrutgiftene fremkommer av forprosjektrapporten, mens anslagene på arbeidsinnsats og lignende er utarbeidet på grunnlag av innhentede kalkyler. Det er usikkerhet knyttet til dette inntill konkrete tilbud eller anbud foreligger. Anslagene er ment å ha tilstrekkelig presisjon til å fungere som grunnlag for beslutninger om prosjektetablering.

Vi har valgt å dele opp dette i tre kategorier:

1. Løsning Alta kommune
2. Løsning Bærum kommune
3. Løsning i regionalt helsenett

1. Løsning Alta kommune

Det er ikke etablert noen form for kommunikasjon mellom sikker og indre sone ved Alta.

Det er heller ikke gitt informasjon om bruk av post tjenester, slik at vi har beregnet et nytt system for sikker sone ved Alta.

Man ser for seg to alternativer for realisering av post sikker sone ved Alta:

- Bruk av tradisjonell post tjeneste ved MS - Exchange.
- Bruk av terminal server basert løsning med MS Exchange

Tradisjonell post tjeneste.

Det må etableres en egen server/tjeneste for post. Her har man valgt å benytte MS Exchange med W2K som plattform.

Type	Pris (eks mva)	Merknader
Server inkl. SW /backup etc	70 500,-	
Lisenser for brukere 15 stk	13 500,-	
Installasjon og tilpassninger	30 000,-	Ca 1 uke
Dokumentasjon/prosjektering/test	15 000,-	
Totalt	129 000,-	

Nettverk:

Type	Pris (eks mva)	Merknader
Checkpoint FW-1	85 000,-	
Maskinvare Checkpoint	51 000,-	
Router Cisco	6 500,-	
VPN terminator	6 000,-	
Konfigurering og installasjon	21 500,-	
Dokumentasjon/prosjektering/test	15 000,-	
Totalt	185 000,-	

Det forutsettes at man har et nettverk basert på Ethernet.

Type	Pris (eks mva)	Merknader
Kommunikasjonslinjer (128kb)	12 000	Eablering
Pr mnd	6 200	
Kommunikasjonslinjer (256kb)	12 000	Eablering
Pr mnd	7 000	

Her er det angitt priser på fast samband fra Alta til Vadsø (tilkobling til Nord Norsk Helsenett)

Bistand fra kommunens IT-avdeling, kan beregnes til ca 2 uke (definering av brukere, postkasser etc)

Type	Pris (eks mva)	Merknader
Informasjonssikkerhet/Datatilsynet	50 000	

Bruk av Terminalserver (Citrix Metaframe)

Det må etableres en egen server/tjeneste for post. Her har man valgt å benytte MS Exchange med W2K som plattform.

Type	Pris (eks mva)	Merknader
Server inkl. SW /backup etc	70 500,-	
Lisenser for brukere 15 stk	13 500,-	
Citrix Metaframe XP	80 000,-	
Installasjon og tilpassninger	30 000,-	Ca 1 uke
Dokumentasjon/prosjektering/test	15 000,-	
Totalt	209 000,-	

Nettverk:

Type	Pris (eks mva)	Merknader
Checkpoint FW-1	85 000,-	
Maskinvare Checkpoint	51 000,-	
Router Cisco	6 500,-	
VPN terminator	6 000,-	
Konfigurering og installasjon	21 500,-	
Dokumentasjon/prosjektering/test	15 000,-	
Totalt	185 000,-	

Det forutsettes at man har et nettverk basert på Ethernet.

Type	Pris (eks mva)	Merknader
Kommunikasjonslinjer (128kb)	12 000	Etablering
Pr mnd	6 200	
Kommunikasjonslinjer (256kb)	12 000	Etablering
Pr mnd	7 000	

Her er det angitt priser på fast samband fra Alta til Vadsø (tilkobling til Nord-Norsk Helsenett)

Bistand fra kommunens IT-avdeling, kan beregnes til ca 2 uke.
 Opplæring og kursing på Citrix Metaframe kommer i tillegg.

Type	Pris (eks mva)	Merknader
Informasjonssikkerhet/Datatilsynet	50 000	

2. Løsning for Bærum kommune

Bærum kommune har planlagt å ta i bruk terminalserver for sikker sone, herunder posttjeneste.

Vi forutsetter at etablering av en posttjeneste på sikker sone er med i WTS prosjektet for Bærum kommune, og at de respektive antall lisenser er på plass.

I tillegg forutsetter man at den indre sikkerhetsbarrieren er på plass.

Type	Pris (eks mva)	Merknader
Nettverkskort Ethernet I FW-1	2 500,-	
Router Cisco	6 500,-	
VPN terminator	6 000,-	
Konfigurering og installasjon	15 000,-	2 dager
Dokumentasjon/prosjektering/test	15 000,-	
Totalt	45 000,-	

Kommunikasjonslinjer

Type	Pris (eks mva)	Merknader
Kommunikasjonslinjer (512b)	15 000	Etablering
Pr mnd	4 200	
Kommunikasjonslinjer (2Mb)	15 000	Etablering
Pr mnd	5 400	

Bistand fra kommunens IT-avdeling, kan beregnes til ca 2 uker (definerer av brukere, postkasser etc)

Type	Pris (eks mva)	Merknader
Informasjonssikkerhet/Datatilsynet	70 000	

3. Løsning for sentralt helsenettverk.

Det forutsettes at det er kommunikasjon mellom de regionale helsenettene. Det etableres en egen DNS server ved et av de to lokasjonene. Denne DNS server har som oppgave å holde rede på de lokale post servere.

Ved en eventuell sammenbinding av de ulike helsenettene, bør denne DNS tjenesten flyttes til det overbyggende nasjonale helsenett, der man også kan etablere flere tjenester som katalog, navnetjeneste etc.

I tillegg forutsette det at man har tilgang til et nytt bein en av de eksisterende sikkerhetsbarrierene, slik at man kan få etablert en DMZ-sone der man plasserer DNS server og VPN terminator.

Man har i denne fasen benyttet de samme VPN terminatorer som er installert hos kommunene. Dersom det blir tilkoblet flere kommuner, vil man anbefale at man benytter en kraftigere VPN terminator sentralt.

Type	Pris (eks mva)	Merknader
DNS-server Maskinvare	50 000,-	
Konfigurasjon/oppkobling/test	21 500,-	3 dager
Router Cisco 2x	13 000,-	
VPN terminator	6 000,-	
Konfigurering og installasjon	15 000,-	2 dager
Dokumentasjon/prosjektering/test	15 000,-	
Totalt	120 500,-	

Bistand fra Helsenett IT-avdeling, kan beregnes til ca 2 uker til oppsett av VPN kanaler gjennom helsenett.

Div tilpasninger og forutsetninger

Det bør taes stilling til navnestruktur og domenenavn dersom man skal koble på flere kommuner og institusjoner til de regionale helsenett

Andre prosjektkostnader

Det er her tatt inn utgifter til prosjektetablering, prosjektledelse, møtevirksomhet, skrivearbeid og lignende.

Prosjektledelse: Arbeidstid prosjektleder : 192 timer a kr. 955,- =
183.360,-

Reiser prosjektleder: 6 i Bærum/6 i Alta = 90.000,-

Felles oppstartsmøte og workshop i Oslo, reiser og møtearrangement =
102.000,-

Sum andre prosjektkostnader: 355.360,-

Denne kostnaden deles i oversikten nedenfor i tre deler mellom Alta og Bærum kommune og helsenettet etter det relative forholdet mellom de tre aktørene når det gjelder ekstern timeinnsats.

Totale prosjektkostnader

Alle priser er veiledende priser eksklusive MVA.

	Nødvendig teknisk utstyr og kjøp	Arbeidsinnsats		Andre prosjektkostnader	Totalkostnad pr aktør
		Ekstern	Intern (timer)		
Alta kommune Sikker e-post alt. 1	232.500,-	93.500,-	80 timer	174.875,-	500.875,-
Alta kommune Sikker e-post alt. 2	312.500,-	93.500,-	80 timer + kurs	174.875,-	580.875,-
Alta kommune Informasjonssikkerhet		50.000,-			50.000,-
Bærum kommune	15.000,-	45.000,- +Infosikkerhet 70.000,-	80 timer	84.164,-	214.164,-
Helsenett	69.000,-	51.500,-	80 timer	96.321,-	216.821,-
Summeringer (Alta, e-postalternativ 1)	316.500,-	310.000,-		355.360,-	981.860,-

Sentrale begreper

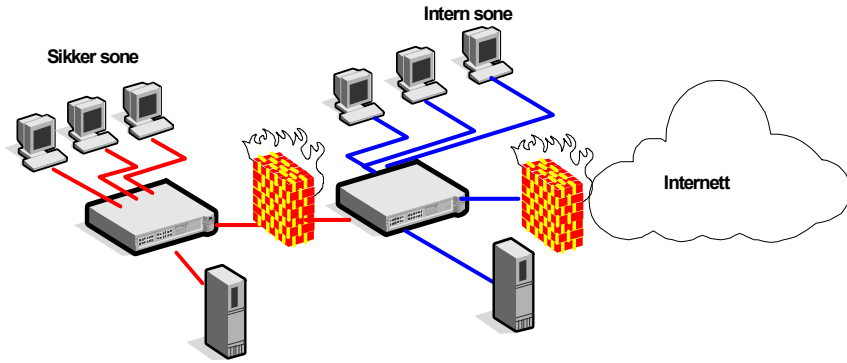
Rapporten er skrevet for lesere med god kjennskap til både informasjonsteknologi og helsevesen. Det kan likevel av og til være vanskelig å ha et klart forhold til hva som legges inn av mening i ord og begreper. Vi har forsøkt å belyse noen av de mest sentrale i denne rapporten.

Sone-begrepet

Et sentral begrep som går igjen i løsninger basert på Datatilsynets ”Veiledning for kommuner og fylkeskommuner” er soner. I denne veiledningen defineres en sone som *”de deler av informasjonssystemet som kan kommunisere ved hjelp av dataoverføring”*. Med dette siktes det til hvordan nettverk og IT-løsninger deles opp slik at kun systemer som har behov for å kommunisere med hverandre kan gjøre det. De begrensninger som sikrer denne inndelingen og dermed deler IT-arkitekturen inn i soner blir betegnet som sikkerhetsbarrierer og kan ha ulike funksjoner. En sikkerhetsbarriere er typisk en brannmur som kontrollerer trafikken på nettverksnivå, men den kan også ha funksjoner på høyere nivå som kontrollerer trafikk og/eller tilgang på system- og applikasjonsnivå.

”Veiledning for kommuner og fylkeskommuner” deler i hovedsak en kommunes nettverk inn i to soner: intern og sikker sone. Intern sone omfatter de deler av kommunens nettverk som f.eks. omfatter løsninger for behandling av administrativ informasjon, kontorstøtte osv., samt ansatte som ikke har behov for tilgang til sensitive personopplysninger. I sikker sone finnes systemer som behandler sensitive personopplysninger og ansatte som har behov for tilgang til disse. I de forslag til nettverksstruktur som presenteres i veiledningen beskyttes intern sone mot eksterne nett som Internett med en sikkerhetsbarriere som bla. hindrer at trafikk initieres inn mot intern sone fra Internett og som har en rekke funksjoner for å filtrere trafikk på nettverksnivå. Sikker sone beskyttes i tillegg av en sikkerhetsbarriere som hindrer trafikk inn fra intern sone. På denne måten er sikker sone skilt fra eksterne nett vha. to sikkerhetsbarrierer.

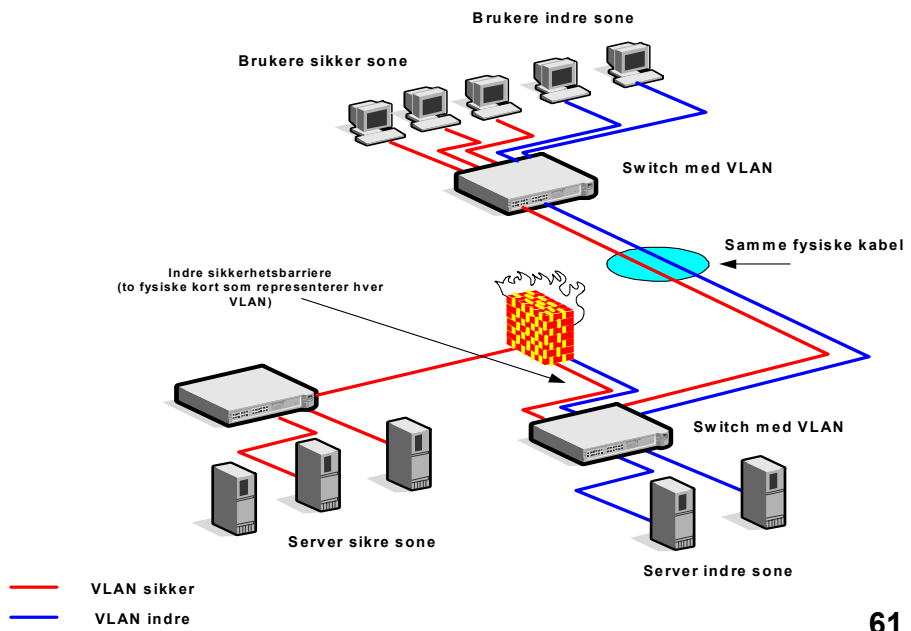
Figur 1 - Eksempel på soneinndeling



VLAN

VLAN (Virtual Local Area Network) er en logisk betegnelse av soner i et nettverk. Trafikken mellom de ulike VLAN er kontrollert i en sikkerhetsbarriere.

Flere VLAN kan overføres i de samme fysiske linjene (kablene) uten at man kan ta del i de ulike VLAN overføringer.

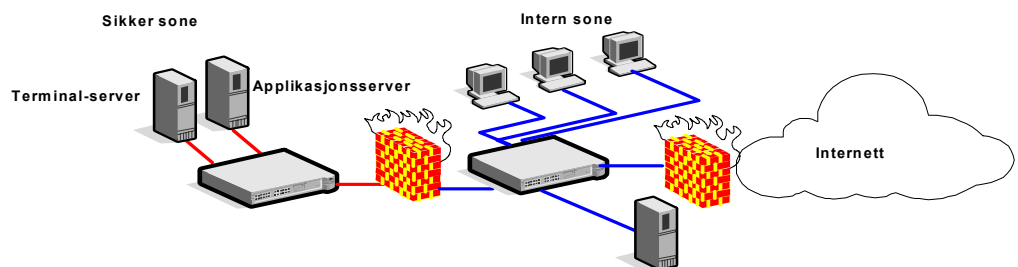


Tidligere måtte man ha to avskilte nettverk (fysisk) for å dekke opp tilsvarende løsning. Bruk av VLAN er en akseptert løsning ref. til veiledninger fra Datatilsynet.

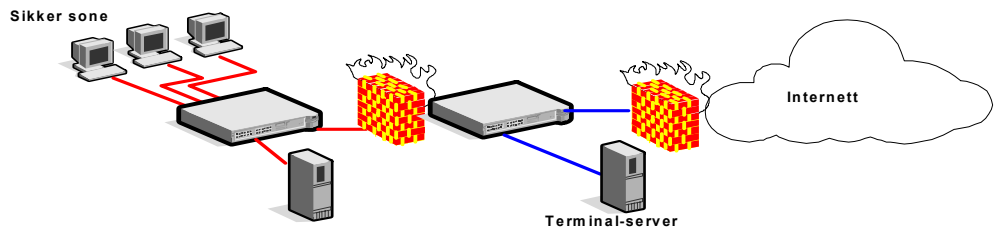
Terminalserver-løsninger

Microsoft Windows Terminalserver er en tynnklient-løsning for systemer med Microsoft Windows operativsystem som tilbyr muligheten for å kjøre applikasjoner på en sentral server mens bilde og musbevegelser/tastetrykk vises/hentes på en arbeidsstasjon. Dette gjør bla. at kravet til prosessorkraft reduseres på arbeidsstasjonen samt f.eks. at applikasjoner kun trenger å oppdateres sentralt. Med tanke på drift av it-løsningen er dette en klar fordel, men i tillegg kan en slik løsning også benyttes for å gi tilgang til systemer samtidig som man hindrer at informasjon flyter mellom applikasjonene f.eks. ved hjelp av klipp og lim. I tillegg som begrepet som beskrevet ovenfor kan dette benyttes for å gi tilgang til internettapplikasjoner som web og epost i sikker sone uten at ondsinnet kode kan skade det lokale systemet, eller for å gi brukere med rettmessig tilgang til sensitive opplysninger tilgang til disse selv om deres arbeidsstasjon er knyttet til en intern sone.

Ved det siste bruksområdet er det viktig at informasjonen fra sensitiv sone ikke kan avlyttes når den går til brukerens arbeidsstasjon i intern sone. Dette kan gjøres med kryptering, noe Citrix Metaframe, en utvidet utgave av Terminalserver, støtter med sin Secure ICA-protokoll. I kombinasjon med en sikker måte å autentisere brukere som skal logge seg på systemet kan dette benyttes enten til å gi brukere lokalisert i intern sone tilgang til applikasjoner med sensitive personopplysninger (figur 1), eller å gi brukere i sikker sone tilgang til applikasjoner som web og e-post på en måte som kan beskytte mot tilsiktet/utisiktet utlevering av sensitive personopplysninger (figur 2).



Figur 2 - Bruk av terminalserver for å gi tilgang til sensitive applikasjoner



Figur 3 - Bruk av terminalserver for å gi tilgang til web/epost

Begrensingene på kommunikasjon som en terminalserver-løsning tilbyr har både positive og negative sider. På den positive siden ligger at faren for utilsiktet utlevering av informasjon, f.eks. gjennom klipp og lim mellom applikasjoner, og muligheten for virus og annen ondsinnet kode som kan gjøre skade kan ramme systemene i sensitiv sone reduseres. På den negative siden kommer bl.a. at typer teknologi som kan brukes i en slik løsning reduseres eller begrenses. F.eks. vil modellen være vanskelig å kombinere med tilgang til videokonferanser over IP da terminalserveren skal overføre skjermbildet fra serveren til arbeidsstasjonen. I tillegg vil det i mange tilfeller likevel være nødvendig å åpne for annen kommunikasjon mellom systemene i sensitiv sone og eksterne nett, f.eks. helsenett bl.a. for meldingsoverføring og annen kommunikasjon.

EDI

EDI står for Electronic Data Interchange, elektronisk datautveksling, og betegner normalt utveksling av informasjon mellom ulike datasystemer på en strukturert og veldefinert måte. Dette innebærer at utvekslingen fortrinnsvis kan foregå uten menneskelig interaksjon, evt. med unntak av å spesifisere hvilken informasjon som skal overføres og evt. kvalitetssikre informasjonen som mottas i systemet. Utvekslingen er strukturert i den betydning at i den grad det er mulig deles informasjonen inn i klart definerte dataelementer som gjør det mulig for mottakerprogrammet å forstå informasjonen som overføres, f.eks. i motsetning til e-post hvor brukeren skriver informasjonen inn i fri tekst og alt overføres i en bulk.

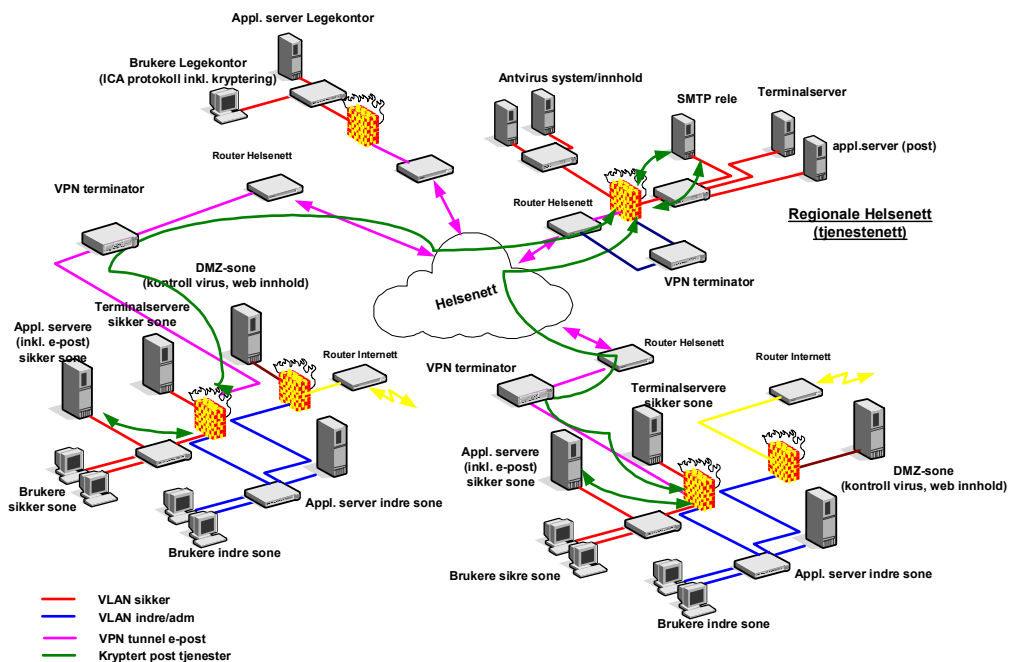
EDI benyttes til slik strukturert informasjonsoverføring i helsesektoren bl.a. til overføring av laboratoriesvar, epikriser osv., som gjør det mulig for en utsendt melding å legges automatisk inn i en leges journalsystem på en slik måte at f.eks. informasjon om diagnosekoder osv. er forståelig for journalsystemet.

Sikker e-post

Med sikker e-post forstår man elektronisk overføring av meldinger inkl. vedlegg via et eller annen kommunikasjonsmedia.

Meldingene blir klassifisert (mht til informasjonssikkerhet) etter de forutsetninger som er gitt i kommunens sikkerhetsinstrukser og fra POL og dets forskrifter (POF).

Det er virksomhetens med det øverste leder som er ansvarlig for at informasjonssikkerhet blir ivaretatt iht til hjemler og forskrifter.



I sikker e-post er følgende er følgende begreper omtalt:

- Bruk av tynne klienter (terminalserverløsning) inkl. kryptering
- Bruk av VPN tunnel med kryptering for overføring av informasjon mellom de ulike postservere.
- SMTP relè ved de regionale helsenett for håndtering av postgang til de ulike postservere

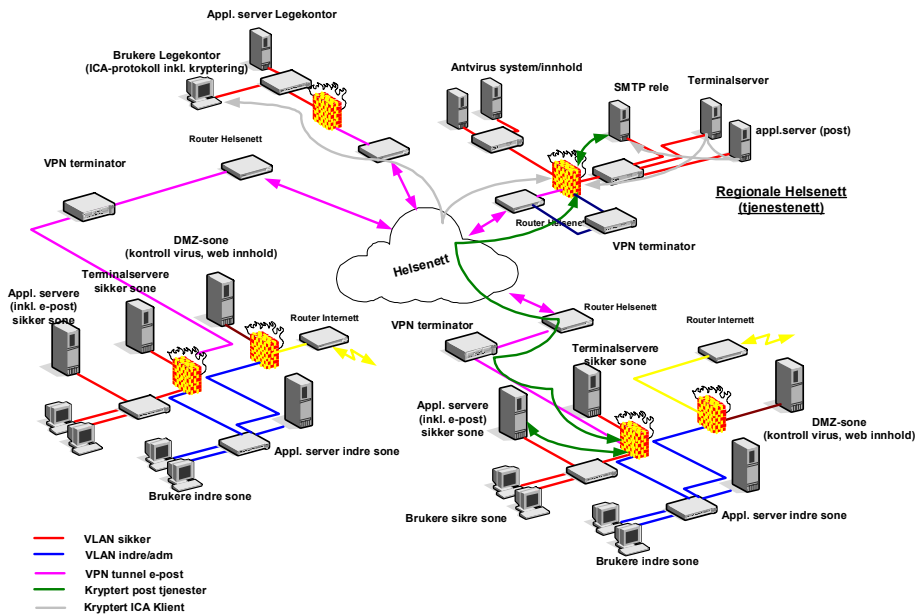
Tynne klienter.

Ref til Terminalserver-løsninger.

Man benytter en 128 bits krypteringsnøkkel som ligger til rette i

Microsoft Windows Terminalserver eller Citrix Metaframe.

Denne løsningen forutsetter at man har etablert en terminalserverbasert e-post tjeneste som blir administrert av helsenett.

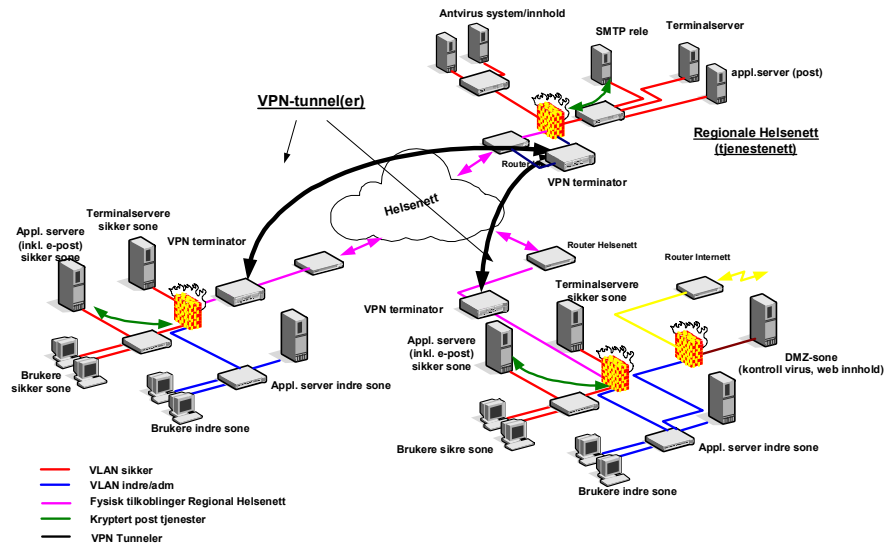


Løsningen er egnet for legekantor(er) og andre institusjoner som ikke har egen postservere.

Bruk av VPN tunnel med kryptering

VPN (Virtual Private Network) er opprettelse av en egen tunnel i et nettverk (LAN og WAN) som blir styrt av IP-adresser og port nummer.

Denne tunnelen settes opp på forhånd før man sender trafikk over nettverket. Man kan i tillegg legge på kryptering (128 b) av trafikken for økt sikkerhet.



Her blir det satt opp en kryptert tunnel mellom de lokasjoner som skal utveksle post.

Tunnelen blir terminert i de lokale terminatorer samt en egen terminator opp mot sentrale tjenester ved de regionale helsenett.

Etter at man har etablert VPN tunnelen kan de to postservere sende og motta post seg imellom.

For at man skal kunne etablere en VPN tunnel over helsenett er det behov en strukturert IP adressering, der de ulike sikkerhetsbarrierer og VPN terminatorer er kjent for hverandre.

SMTP relè

Dette er en standard tjeneste for utveksling av informasjon mellom de ulike postservere som er tilknyttet helsenett, samt opp mot evt fremtidig Internett's e-post tjeneste.

Det kan være flere SMTP relè i nettverket, der man definerer en som den overordnede dersom man skal tilknytte flere regionale SMTP relè til en felles sentrale relè tjeneste.

Intranett

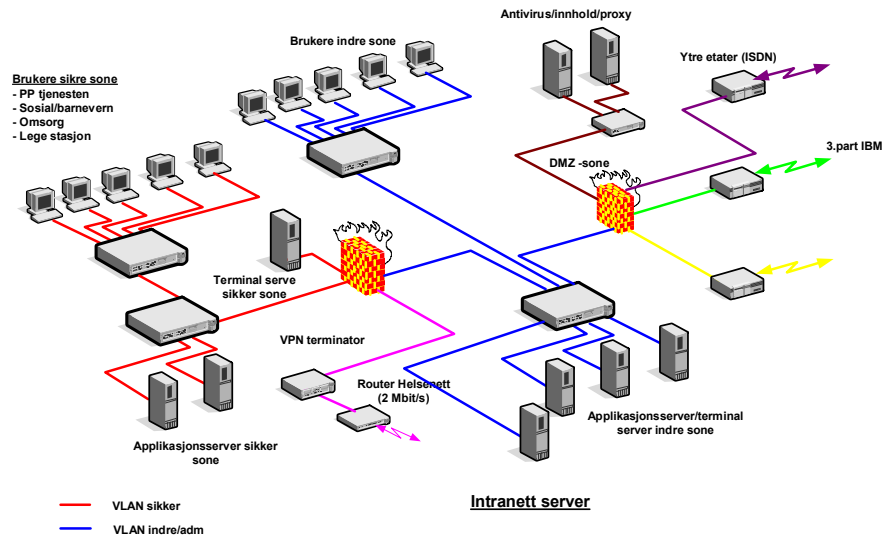
Flere bedrifter og organisasjoner har tatt i bruk Intranett for intern spredning av intern informasjon.

Dette kan være en web basert løsning som kun kan nås fra innsiden av nettverket (internt i virksomheten).

Her kan man legge ut alle interne aktiviteter, telefonkataloger, større aktiviteter samt ulike skjema som de ansatte benytter (søknad ferie, km

lister, reisregningsmaler, interne spørreundersøkelser, ansatt registre med funksjoner etc)

Intranett er en formidler av informasjon mellom de ulike etater/avdelinger innenfor en bedrift, samt mellom de ansatte og ledelsen.



Intranett nås fra den lokale web leseren på hver arbeidsplass. Tjenesten er tilgjengelig fra alle de interne sonene i nettverket.

Prosjektdirektiv

Formål.

Formålet er å foreslå tekniske løsninger for oppkobling av pleie- og omsorgstjenestene i Alta og Bærum kommuner til sine respektive regionale helsenett på en slik måte at det ivaretar krav til god informasjonssikkerhet. Løsningene må være kostnadseffektive og samtidig ivareta behovet for en funksjonell kommunikasjon mellom sykehus, legekantor og omsorgstjeneste. Løsningene skal være overførbare til andre kommuner.

I tillegg skal prosjektet vurdere organisatoriske sikkerhetsprosmål og eventuelt foreslå tiltak for å oppnå tilfredsstillende informasjonssikkerhet i Alta kommune.

Prosjektet skal også planlegge gjennomføringen av de foreslåtte tiltak i form av en prosjektplan for et hovedprosjekt.

Organisering

Prosjektet er et samarbeidsprosjekt mellom Sosial og helsedirektoratet og hhv Alta kommune og Bærum kommune. Det etableres en prosjektgruppe for gjennomføring på oppdrag for direktoratet. Prosjektleder rapporterer til koordinator for program Nasjonalt helsenett i Sosial og helsedirektoratet, Inger Elisabeth Kvaase.

- Prosjektleder: Tormod Hofstad, KITH
- Prosjektdeltakere KITH:
 - ✓ Arnstein Vestad,
 - ✓ Olaf Berglihn,
- Sekretær: KITH

Prosjektgruppe Alta:

- Arnstein Vestad
- Daniel Haga
- Ernst Robert Mortensen

Prosjektgruppe Bærum

- Olaf Berglihn

- Eva Benedicte Liahjell
- Gunvor Erdal
- Per Chr. Solli
- Siri Opheim

I tillegg vil det kunne bli aktuelt å utvide prosjektgruppene med andre personer i enkelte spørsmål.

Referansepersoner

- Gunn Hilde Rotvold, NST
- Sissel Sunde Tveit, Bergen kommune
- Jan Tore Bosåen, Østnorsk Helsenett
- Morten Amundsen, Nordnorsk Helsenett

Prosjektet organiseres i to prosjektgrupper, en for hver kommune, med hhv. Arnstein Vestad og Olaf Berglihn som hovedansvarlig for de respektive arbeidsgruppene.

Hovedtyngden av det utførende arbeidet utføres av KITH. KITH kan eventuelt ved behov kjøpe nødvendig kompetanse fra andre innenfor de avtalte rammene for prosjektet.

Det inngås en avtale mellom Sosial- og helsedirektoratet og KITH om oppdrag/finansiering av bistand og reiseutgifter. Alta kommune kan få dekket noe timeinnsats i prosjektet. Deltagere fra Bærum kommune finansierer egen innsats i prosjektet.

Programleder eller koordinator i Nasjonalt Helsenett kan om ønskelig delta i arbeidsgruppens møter.

Prosjektbeskrivelse

Bakgrunn for prosjektet

Formålet med å etablere regionale helsenett er å etablere en sikker og formålstjenlig infrastruktur for elektronisk samhandling i helsevesenet, samt å kunne tilby aktørene i helsevesenet standardiserte tjenester over nettet som for eksempel telemedisinske tjenester, videobaserte tjenester, katalogtjenester og sikker tilgang til Internett. I definisjonen av helsevesenet inngår også den kommunale helse og omsorgstjenesten. Helsenettene har til nå hatt størst fokus på å koble opp sykehus og primærlegetjenesten. Det vil i økende grad være fokus på å inkludere hele kommunehelsetjenesten som også inkluderer den kommunale omsorgstjenesten, både for å tilby en sikker infrastruktur og for å være premissgiver for tjenesteutvikling.

Mange kommuner har bygd opp interne nett som håndterer utveksling av alle typer informasjon. En må i utgangspunktet anta at kommunene har

løst egen sikkerhetsproblematikk, men på forskjellige måter. Datatilsynet har i forhold til den gamle personopplysningsloven utarbeidet en veileder i informasjonssikkerhet for kommuner og fylkeskommuner.

Kommunalt ansvar.

I utgangspunktet er det kommunens ansvar å sørge for tilstrekkelig sikkerhet i egne systemer til at de kan kobles på helsenett uten at det medfører økt risiko for andre aktører. Det er også lite ønskelig at overordnet myndighet instruerer kommunene om hvordan de konkret skal løse den beskrevne problematikken. Det er likevel av interesse å vurdere sikkerhetsløsninger i helsenettet og internt i kommunen i sammenheng når en søker å nå målsettingen om å inkludere kommunal helse og omsorgstjeneste i helsenett. Dette vil gi verdifull innsikt både for kommunene selv, helseforetakene og andre aktører i det videre arbeidet.

Sikkerhetsproblematikk.

Sikkerhetsproblematikk i forbindelse med bruk av IT-systemer i pleie- og omsorgstjenesten, relatert til tilkobling til helsenett, er et området som det har vært lite fokus på. En har god kjennskap til sikkerhetsproblematikk generelt i helsevesenet, men det har vært arbeidet lite innenfor dette tjenesteområdet. For å få et bedre grunnlag for å gå videre med tiltak ønsker Sosial- og helsedirektoratet innenfor rammene av Nasjonalt Helsenett program gjennom dette prosjektet å belyse sikkerhetsproblematikken i to kommuner med ulik størrelse og infrastruktur og komme med konkrete forslag tiltak på området og prøve disse ut i praksis.

Tre aktører og helsenett.

Utveksling av informasjon i helsevesenet skjer mellom svært mange og ulike aktører.

I denne sammenheng ønskes problematikken avgrenset til tre sentrale aktører; Sykehuset (Spesialisthelsetjenesten), Legekontoret (Primærlegetjenesten) og Omsorgskontoret (Pleie og omsorgstjenesten). Dette er aktører med stort behov for samhandling og det prioriteres derfor oppkobling av kommunene mot helsenett skal ivareta sikker kommunikasjon mellom disse tre aktørene.

Hensikt med prosjektet

- Prosjektet skal foreslå konkrete løsninger for tilkobling til respektive regionale helsenett i kommunene Alta og Bærum. Disse løsningene skal tilfredsstillende krav til informasjonssikkerhet og samtidig være funksjonelle og kostnadseffektive. Med funksjonalitet nevnes spesielt ønsket om at løsningene legger til rette for sikker tilgang til Internett og sikker e-post. Løsningene skal være overførbare til andre kommuner.
- De to konkrete løsningene skal inneholde kostnadsoverslag.
- Alta kommunes organisatoriske informasjonssikkerhet skal vurderes og eventuelle tiltak foreslås. Tiltakene skal være kostnadsvurderte.
- Prosjektet skal i tillegg planlegge og foreslå et hovedprosjekt for oppkobling av disse to kommunene til helsenett.

Prosjektets leveranser

- Prosjektet skal levere en sluttrapport som inneholder løsningsforslag for oppkobling av Alta og Bærum kommuner til hhv Nordnorsk Helsenett og Østnorsk Helsenett, inklusive kostnadsoverslag.
- Sluttrapporten skal beskrive status på organisatoriske sider ved informasjonssikkerheten i Alta kommune, og om nødvendig foreslå tiltak for forbedring med kostnadsfastsettelse.
- Det skal i tillegg leveres forslag til prosjektplan for et hovedprosjekt for oppkobling av de to pilotkommunene, samt eventuell gjennomføring av tiltak for bedring av organisatorisk informasjonssikkerhet.

Konkrete mål som skal realiseres i prosjektperioden

Konkrete forslag.

Det skal i forprosjektet taes utgangspunkt i to kommuner: Alta og Bærum. Disse representerer ulik størrelse, kompleksitet og erfaring med IT-løsninger. De har også naturlig tilknytning til to lokalsykehus og to regionale helsenett. Dette vil kunne gi grunnlag for å komme med konkrete anbefalinger som kan anvendes i andre kommuner.

Vi ønsker spesielt at det blir sett på følgende tekniske (Alta og Bærum) og organisatoriske forhold (Alta) knyttet til informasjonssikkerhet:

Tekniske forhold som skal vurderes:

- hvordan det fysiske nettet er strukturert i forhold til resten av kommunens nettverk
- hvordan skillet mellom systemer som håndterer helseopplysninger og andre systemer er håndtert
- hvordan tilgangskontroll er håndtert
- tekniske sikkerhetsbarrierer som er etablert (brannmurer etc)
- hvordan eventuell tilkopleing mot Internett er etablert
- om det er i bruk terminalløsninger
- om det er tatt i bruk, eller om det foreligger planer for å ta i bruk mobile løsninger eller håndholdt utstyr
- hvordan virusproblematikken håndteres
- om det er planer om å ta i bruk PKI-løsninger

Organisatoriske forhold som skal vurderes:

- hvordan sensitiv personopplysninger behandles i dag og i hvilke systemer slik informasjon behandles
- hvilke eksterne aktører sensitive personopplysninger utveksles med
- hvordan gjeldende lovgivning (personopplysningsloven med forskrifter) ivaretas
- ansvarlinjer for informasjonssikkerheten og behov for revisjon, eventuelt etablering av sikkerhetspolicy
- behov for å gjennomføre sikkerhetsrevisjoner
- hva som er gjort i forhold til risikovurderinger (f.eks. i forbindelse med år 2000 arbeidet)

Forprosjektet skal avsluttes med:

- utarbeiding av tekniske løsninger for Alta og Bærum.
- forberedelser til eventuell inngåelse av rammeavtaler
- vurdering av kostnader
- utarbeiding av eventuelle forslag til organisatoriske tiltak for informasjonssikkerhet i Alta kommune.

Planlegging av hovedprosjekt.

En vil søke å etablere et hovedprosjekt for oppkobling av kommunal omsorgstjeneste og primærlegetjeneste i Alta og Bærum til sine regionale helsenett.

Forprosjektet skal lage en prosjektplan for dette hovedprosjektet. I prosjektplanen inngår et forslag til økonomiske rammer for hovedprosjektet. Prosjektplanen skal danne grunnlag for nærmere avklaringer av økonomiske spørsmål i hovedprosjektet.

Sammenheng med andre prosjekter

Prosjektet inngår i Nasjonalt Helsenett program, hvor det er knyttet opp mot følgende tiltak i programplanen i "Si @!":

- Statlige tiltak – utbygging av infrastruktur: Førstelinjen skal kunne knytte seg til helsenettet i regionen.
- Statlige tiltak – utvikling av basistjenester: Utvikle og formidle prinsipper og krav til håndtering av sikkerhet hos aktørene i helsenettet som ivaretar gjeldende lover og regelverk for personvern og datasikkerhet i sektoren.

Prosjektet bør videre søkes samordnet med erfaringsgrunnlaget i fire prosjekter:

- Kartlegging av IT-løsninger i kommunal sektor. (KS/Norsk Gallup)
- Kartlegging av informasjonsutveksling mellom kommunal pleie- og omsorgstjeneste og andre aktører i helsevesenet, samt utvikling av de fem høyest prioriterte meldingstjenestene for omsorgstjenesten. (SHD/NST.)
- Standard for dokumentasjonssystemer i pleie og omsorgstjenesten. (SHD/KITH)
- Sammenkobling av Midtnorsk Helsenett og Nordnorsk Helsenett. (Nasjonalt Helsenett/KITH/NNH .)

Ressursanslag

- Varighet (måneder): 3 – avsluttes 01.05.2002
- Dagsverk:
 - KITH: 53

➤ **Kostnadsanslag:**

- KITH:386.000,- (424 timer a 910,-) + administrative kostnader på 60.000,- (i hovedsak reisekostnader: 3 reiser Alta ca 30.000,-, 3 reiser Bærum ca 15.000,-, og ett prosjektmøte i hver av prosjektgruppene ca 15.000,-)
- Dekning av timeinnsats Alta: Pr time, a 250,- avgrenset oppad til kr. 25.000,-
- Sum.471.000,- kr

Alle kostnader er eks. mva.

Prosjektplaner - Statusrapportering

Det skal utarbeides prosjektplan for prosjektet. Prosjektleder er ansvarlig for dette.

Det skal om ønskelig rapporteres månedlig fra prosjektleder til koordinator i Sosial- og helsedirektoratet for program Nasjonalt Helsenett.

Prosjektet er formelt godkjent den

Inger Elisabeth Kvaase
Seniorrådgiver Sosial- og helsedirektoratet

Knut Krane
Rådmann Alta kommune

Elisabeth Enger
Rådmann Bærum kommune

Intervjuguide og spørreskjema



Intervjuguide

SJEKKLISTE ALTA OG BÆRUM.

Shdir-SKN02

NAVN	STILLING/FUNKSJON	TID	STED
------	-------------------	-----	------

1. ORGANISATORISKE FORHOLD (Bærum kommune)

1.1	Hvor utstrakt er behandlingen av sensitiv personopplysninger? Her i betydningen elektroniske systemer som helseregistre, elektroniske rapporter og lignende. Antall pasienter registrert, antall brukere av systemet.
1.2	I hvilke systemer behandles slik informasjon? Type system, navn, leverandør, innført når?
1.3	Til hvilke eksterne aktører kommuniseres sensitive personopplysninger? Hvilke institusjoner: sykehus, legekontorer, trygdekontor osv. Evt hvilke <u>ønsker</u> en å utveksle informasjon med? Omfanget av informasjonsutvekslingen? Hyppighet, antall pasienter?
1.4	Hvor godt kjenner man til gjeldende lovgivning? (Personopplysningsloven med forskrifter) Hvem kjenner til krav, hvem er ukjent med loven/inholdet?

1.5	Hvem i kommunen har ansvaret for informasjonssikkerheten? Hvordan håndteres dette ansvaret i praksis?
1.6	Er det etablert en sikkerhetspolicy? Hvilke tjenesteområder/institusjoner o.l omfattes av denne?
1.7	Hva inneholder denne sikkerhetspolicyen? Kan vi få tilgang til det skriftlige materialet?
1.8	Er det gjennomført sikkerhetsrevisjoner? Internkontroll og/eller ekstern revisjon?
1.9	Er det gjennomført noen risikovurderinger av IT-systemer? (f.eks ved år 2000 arbeidet)
1.10	Hvem har ansvar for IT-driften? Internt eller eksternt?

2.	TEKNISKE FORHOLD. (Alta og Bærum kommune)
-----------	--

2.1	Hvordan er det fysiske nettet strukturert ift til resten av kommunens nettverk? Er det utarbeidet modeller/kart?
2.2	Hvordan skiller man systemer (innen helse/omsorg) som håndterer helseopplysninger fra andre systemer? Innloggingsmekanismer, tilgangsstyring, oppdeling av nett/soner, brannmurer.
2.3	Hvordan håndteres tilgangskontrollen? Rutiner.
2.4	Hvilke tekniske sikkerhetsbarrierer er etablert (brannmurer etc)?
2.5	Er det etablert tilkobling mot Internett? Hvem har tilgang, hvordan styres denne, hvordan hindres uvedkommendes tilgang til egne sensitive pers.oppl. ? Foreligger det planer om etablering av internettilgang?
2.6	Brukes terminalløsninger?
2.7	Er det tatt i bruk, evt planlagt, mobile løsninger eller håndholdt utstyr? (som gir tilgang til sensitive personopplysninger)
2.8	Hvordan håndteres virusproblematikken?
2.9	Er det planer om å ta i bruk PKI-løsninger?

Notater/svar på spørsmål tas ned på egne ark under samtalen. Behold og bruk nummereringen.

Spørreskjema med følgebrev

KITH

Sukkerhuset

7489 Trondheim

Trondheim 13.05.2002

NN

XX kommune

SPØRRESKJEMA OM PRIORITERING AV TJENESTER/FUNKSJONALITET I FORBINDELSE MED TILGANG TIL HELSENETT.

I prosjekt *Forprosjekt for løsningsspesifikasjon for tilkobling av Alta og Bærum kommuner til helsenett* er vi nå kommet til et punkt hvor en må avklare kommunenes egne prioriteringer. Spørsmålet dreier seg om hvilke tjenester kommunen, dvs pleie- og omsorgstjenesten, ønsker å få tilgang til når en tilkobles helsenett. Dette legger føringer for de løsninger som må etableres for å oppnå tilfredsstillende grad av sikkerhet.

En viktig avgrensning er lagt i prosjektets direktiv. Der defineres pleie- og omsorgstjenestens viktigste samarbeidspartnere, her i betydningen de aktører det er viktigst å motta og/eller avgi informasjon til, til å være legekantoret og sykehuset. Andre aktuelle samarbeidspartnere, som for eksempel apotek og trygdekantor, er ikke ment å være uten betydning, men er i dette prosjektet ikke vektlagt så mye at løsningene vil bli

utarbeidet med disse som fokus.

Med utgangspunkt i tidligere erfaring fra helsesektoren har vi har tillatt oss å foreslå en inndeling og opplisting av tjenester vi mener er hensiktsmessig og aktuelt for pleie- og omsorgstjenesten. Vi har også gjort en vurdering av hva som er tilgjengelige tjenester i helsenett pr. dato og i nær framtid, og av hva som er tilgjengelig teknologi. Vi gjør oppmerksom på at det er pleie- og omsorgstjenestens behov (Ikke legetjenestens eller legekantorets behov) vi ønsker en vurdering av, og at vi ber om både omsorgstjenestens egen vurdering (ved leder for tjenesteområdet) og medisinsk ansvarliges vurdering.

Vi ber deg om å prioritere de foreslåtte tjenester med utgangspunkt i din vurdering av pleie- og omsorgstjenestens behov. Det gjør du ved å sette ett tall foran hver tjeneste med stigende tallverdi fra 1 til 3. 1 er høyeste prioritet, 3 er laveste prioritet. Du må altså velge en verdi for alle tjenestene, men kan gi samme verdi til flere tjenester.

Vi må dessverre gi en kort tidsfrist på besvarelsen. **Vi må ha svaret tilbake som vedlegg til e-post fra deg i løpet av torsdag 16 mai.** Det betyr at vi ikke forutsetter en omfattende avklaringsprosess internt i kommunen, men at det er dine egne faglige og administrative vurderinger og synspunkter som må legges til grunn. Vi gjør oppmerksom på at likelydende spørreskjema er sent tilog ater informert om at dere har mottatt dette spørreskjemaet til besvarelse.

PRIORITET (Sett tall fra 1 til 3)	TJENESTE
	Sikker e-post (inkluderer mulighet for sensitiv personinformasjon)
	Usikker e-post (inkluderer ikke personsensitiv informasjon)
	Tilgang til definerte adresser på Internett (for eksempel oppslag i helserelevante databaser)
	Begrenset tilgang til Internett (åpen tilgang for ansatte med definert behov)
	Åpen tilgang til Internett (for alle ansatte)

	Standardiserte meldingstjenester med pasientinformasjon (som for eksempel epikrise, sykepleieinformasjon ved utskrivning av pasient fra sykehus, medisineringskjema ol)
	Tilgang til administrativ informasjon (som for eksempel saksbehandlingsverktøy, lønn/personal og budsjett/regnskapssystemer)
	Bookingsystemer (for bestilling av time hos lege eller på poliklinikk, reservasjon av tidspunkt for bestemte undersøkelser og lignende)

I tillegg ber vi deg om å skrive inn kommentarer eller annet du mener har interesse for problemstillingen her (For eksempel tjenester vi ikke har nevnt og som har verdi for pleie- og omsorgstjenesten.)

Annet:

Vennlig hilsen Tormod Hofstad
 Prosjektleder
tormod.hofstad@kith.no