

Oppsummering av sikkerhetskritiske aspekter



SES@m Tromsø

Telemedisin i pleie- og omsorgstjenesten
Fyrtårnsprosjekt for bedre samordning og
kontinuitet i helsesektoren

Det kan fritt kopieres fra denne publikasjonen hvis kilden oppgis. Brukeren oppfordres til å oppgi rapportens navn, forfatter, samt at den er utgitt av Nasjonalt senter for telemedisin og at den i sin helhet er tilgjengelig på www.telemed.no.

© 2006 Nasjonalt senter for telemedisin

Innhold

1	Innledning	4
1.1	Om dokumentet og målgruppen	4
1.2	Forfattere	4
2	Sammendrag og hovedkonklusjoner	5
2.1	Oversikt over løsningene	6
2.1.1	<i>Det teknologiske utgangspunktet</i>	6
2.1.2	<i>Endringer i kommunens infrastruktur</i>	6
2.1.3	<i>Endringer og nye programmer</i>	7
2.1.4	<i>Mobil tilgang</i>	9
2.2	Viktigste trusler	9
2.2.1	<i>Passordhåndtering</i>	9
2.2.2	<i>Integrasjon av kommunikasjon i fagsystemet</i>	9
2.2.3	<i>Enklere sikker tilgang fra mobile klienter</i>	11
3	Tilkobling til helsenettet og nye tjenester	12
3.1	Teknisk infrastruktur og tilkobling til helsenettet	12
3.2	Elektronisk kommunikasjon	13
3.3	Viktigste trusler	13
3.3.1	<i>Trusler med høyt risikonivå</i>	13
3.3.2	<i>Trusler med lavt risikonivå</i>	16
4	Mobil løsning	18
4.1	Oppbygning og konfigurering	18
4.1.1	<i>Utfordringer ved flere brukere på bærbare datamaskiner</i>	19
4.2	Prosess for pålogging og autentisering	19
4.3	Sikkerhetsfaktorer og sentrale trusler	22
4.3.1	<i>Autentisering, passord osv</i>	22
4.3.2	<i>Tap av mobilt utstyr</i>	23
4.3.3	<i>Hacking og ondsinnet kode</i>	23
4.3.4	<i>Manglende tilgang</i>	24
4.3.5	<i>Avlytting av mobil forbindelse</i>	24
5	Brukeraspekter	25
5.1	Passord	25
5.2	Utskrift	25
5.3	Dårlig eller manglende tilgjengelighet	26
5.4	Organisatoriske aspekter	27
5.4.1	<i>Oppfølging av meldinger (feil og innkommende)</i>	28
5.4.2	<i>Urettmessig tilgang til (administrative) pasientopplysninger</i>	31
5.4.3	<i>Manglende oppfølging fra fastleger</i>	31
5.4.4	<i>Tap av kamera/kameraminnekort</i>	32
6	Forkortelser	33
7	Referanser	34

1. Innledning

1.1 Om dokumentet og målgruppen

Formålet med prosjektet SES@m Tromsø var å sikre bedre samordning og kontinuitet i helseffelsektoren og å bidra til en helhetlig og samordnet tjeneste med fokus på kontinuitet og kvalitet ved elektronisk samhandling mellom de ulike enhetene og nivåene i helsesektoren. Prosjektperioden var 1.1.2004 – 30.6.2006.

Dette dokumentet er en oppsummering av informasjonssikkerhetsmessige aspekter som har vært vurdert i forbindelse med løsningene som har blitt implementert og/eller testet ut i SES@m Tromsø-prosjektet. Flere risikovurderinger har vært gjennomført for å utrede mulige sikkerhetstrusler relatert til løsningene og bruken av dem. Risikovurderingene førte til fortløpende anbefalinger om tiltak og endringer for å sikre et akseptabelt risikonivå. Dette dokumentet er utarbeidet på bakgrunn av resultatene fra disse risikovurderingene. Vi har valgt å presentere de delene som kan være av generell interesse for andre. Dokumentet er basert på utprøving av spesifikke produkter og løsninger, men vi har forsøkt å trekke ut det som antas å være av generell interesse uavhengig av enkeltprodukter. Dokumentet må sees i sammenheng med andre leveranser i SES@m Tromsø-prosjektet.

For en mer detaljert beskrivelse av løsningene, hvorfor vi landet på de løsningene vi gjorde og hvorfor vi gikk bort fra andre tiltenkte løsninger, henvises det til dokumentene ”Teknisk dokumentasjon” og ”Tekniske erfaringer”. Se kapittel 7 Referanser.

1.2 Forfattere

Nasjonalt senter for telemedisin (NST) har utarbeidet dette dokumentet i samarbeid med Tromsø kommune. Forfattere: Eva Skipenes, NST, og Arnstein Vestad, KITH. I tillegg har følgende bidratt fra NST: Harald Øverli Eriksen, Daniel Nygård og Line Nordgård. Fra Tromsø kommunes IT-avdeling har Roger Hansen og Frank Johansen bidratt.

2. Sammendrag og hovedkonklusjoner

Ved oppstart av SES@m-prosjektet var Tromsø kommune knyttet opp mot Norsk Helsenett (NHN) via en fiberring i kommunen, men det var kun legevakta og sosialmedisinsk senter som benyttet seg av denne tilkoblingen. I løpet av SES@m-prosjektet ble det tatt i bruk løsninger for å kommunisere mellom helsepersonell i pleie- og omsorgssektoren i kommunen, fastleger og Universitetssykehuset i Nord-Norge (UNN) via helsenettet. Helsepersonellet i kommunen ble også gitt tilgang til en elektronisk prosedyrebank i Helse Nord, og enkelte grupper tok i bruk bærbare datamaskiner med mobil tilgang til kommunens nett for å kunne gjøre oppslag og kommunisere elektronisk ute hos pasientene.

Alle disse endringene medførte behov for risikovurderinger med formål å kartlegge trusler og risikofaktorer ved de nye løsningene. Alt i alt ble det gjennomført 3 risikovurderinger i løpet av SES@m-prosjektet:

- Risikovurdering av mobil tilgang til fagapplikasjoner i Tromsø kommune
- Risikovurdering av løsningene i SES@m-prosjektet fra et brukerperspektiv
- Risikovurdering av tekniske løsninger for å realisere elektronisk kommunikasjon i SES@m-prosjektet

Både risikovurdering av tekniske løsninger og vurdering fra brukerperspektiv ble gjennomført i to omganger, i startfasen og ved slutten av prosjektet.

Det sikkerhetsmessige utgangspunktet for prosjektet var at de nye løsningene og tjenestene som ble innført skulle oppfylle lovpålagte krav til sikkerhet for behandling av sensitive personopplysninger. Disse kravene innebærer bl.a. at personopplysningene skal være tilgjengelig for de som er autorisert for det, og som i tillegg har et tjenestelig behov for tilgang til opplysningene, når de trenger dem. Opplysningene skal ikke være tilgjengelig for andre.

Dette kapitlet gir en oversikt over løsningene som ble valgt/utarbeidet av SES@m-prosjektet, og oppsummerer de viktigste sikkerhetsmessige risikofaktorene. De neste kapitlene ser nærmere på resultater fra de gjennomførte risikovurderingene, beskriver løsningene nærmere og trekker fram de viktigste resultatene fra vurderingene.

I dette dokumentet fokuserer vi i hovedsak på de endringer som er gjort i risikobildet for Tromsø kommune på bakgrunn av de tekniske og organisatoriske endringene som er en direkte følge av SES@m-prosjektet. Vi vil likevel nevne innledningsvis at manglende bruk av pleieplaner og modul for daglig rapportering i det elektroniske journalsystemet i kommunen, samt manglende integrasjon av meldingskommunikasjon i journalsystemet, er medvirkende årsak til svært mange av truslene vi fant i risikovurderingene. Vi imøteser implementeringen og videreutviklingen av PLO-standard som KITH har utviklet. Målet må være at kommunikasjonen skal gå fra journalsystem til journalsystem, og at kommunikasjonsprogramvaren kun skal ta seg av sikker meldingstransport uten noe direkte brukergrensesnitt, bortsett fra for avvikshåndtering.

Hovedkonklusjonen fra arbeidet med sikkerhet og risikovurdering av løsningene i

SES@m-prosjektet bør ikke komme som en overraskelse for personer med erfaring med sikkerhetsarbeide. De viktigste risikofaktorene som ble avdekket, konsentrerer seg rundt ulike brukeraspekter. Mens det ved å følge retningslinjer for sikker programutvikling er mulig å komme fram til teknisk ”sikre” løsninger, f.eks. løsninger som beskytter mot ond-sinnet kode, inntregning i datanettverket osv. – er det større utfordringer knyttet til sikker bruk, f.eks. passordrutiner, kontroll og oppfølging av avvik osv. Etablering av mobil tilgang til kommunens fagsystemer innebar likevel en del teknologiske utfordringer for å få til en sømløs og brukervennlig autentiseringsløsning på tvers av mange ulike teknologier (bær-bar datamaskin, mobilnett, Internett, brannmur, terminal-serverløsning, etc).

Når det gjelder sikkerhetsmessige utfordringer vil vi i dette dokumentet trekke fram behovet for sikre metoder for å autentisere brukere, som er både enkle og effektive for brukerne, behovet for å integrere kommunikasjon i helsearbeidernes fagsystemer og problemer knyttet til Norsk Helsenetts bruk av ip-adresser fra private ip-ranger for sine kunder.

For utdypende beskrivelser av de tekniske løsningene og valg som ble gjort underveis i SES@m Tromsø-prosjektet henviser vi til dokumentene ”Teknisk dokumentasjon” og ”Tekniske erfaringer”. Se kapittel 7 Referanser.

2.1 Oversikt over løsningene

2.1.1 *Det teknologiske utgangspunktet*

Datamaskiner på vaktrom på sykehjem og i hjemmetjenestene var fra før av koblet opp mot kommunens nettverk via en terminalserverløsning. Kommunen hadde tidligere valgt å innføre det elektroniske journalsystemet Profil fra Visma Unique som fagsystem for pleie- og omsorgssektoren. Det var kun de administrative delene av fagsystemet med opplysninger om pasientenes navn, adresse, fødselsdato o.l. og hvilke tjenester de mottok av kommunen, som var tatt i bruk. Modulene for pleieplaner og daglig rapportering ble ikke brukt. Hver enkelt enhet i sektoren hadde papirjournaler for den daglige oppfølgingen av pasientene. Kommunikasjon med fastleger, tilsynsleger og sykehus foregikk pr telefon og brev. Kommunen hadde planer om å ta i bruk modulene for pleieplaner og daglig rapportering i Profil i løpet av SES@m-prosjektet, men dette ble ikke gjort.

De ansatte i pleie- og omsorgssektoren hadde tilgang til e-post og Internett ved pålogging til intern/åpen sone i kommunens nett fra datamaskiner på vaktrom på sykehjem og i hjemmetjenestene. I denne sonen var det ikke tillatt å håndtere sensitive pasientopplysninger.

I resten av dokumentet har vi benyttet begrepene fagapplikasjon, fagsystem eller journalsystem når vi skriver om journalsystemet Profil.

2.1.2 *Endringer i kommunens infrastruktur*

Ved oppstart av SES@m-prosjektet ble det etablert kommunikasjon fra pleie- og omsorgssektoren ut av kommunens nettverk. Kommunikasjonen fra Tromsø kommune til UNN og fast-/tilsynslegene gikk over kommunens tilknytning til Norsk Helsenett, gjennom en VPN-tunnel. Denne tunnelen startet fra en VPN-router i NHN og endte i en VPN-router som stod på et eget VLAN på Tromsø kommunes indre brannmur. Begge disse VPN-routerene

var kontrollert av NHN. Legekontorer var koblet opp til NHN på samme måte som Tromsø kommune.

Samhandlingen ved hjelp av asynkron meldingsutveksling mellom Tromsø kommune, UNN og fast-/tilsynslegene foregikk ved hjelp av postkassemodellen. Hvis EDI-serverne hos NHN var navet i hjulet, var kommunikasjonspartnerne i prosjektet eikene. Alle meldinger ble lastet opp og hentet ned fra EDI-serverne hos NHN. Dette ble gjort ved at hver enkelt partner initierte kontakt fra insiden av sitt nettverk ved hjelp av protokollene SMTP (meldinger ut) og POP (meldinger inn).

Tromsø kommune hadde Microsoft Server 2003 domener i både sikker og intern sone. Dette betyr at Active Directory domene-kontroller i begge soner kjørte operativsystemet Microsoft Server 2003. Alle database-servere, Citrix Metaframe-servere og EDI-serveren kjørte også operativsystemet Microsoft Server 2003. Se Figur 1 i kap. 3.1.

Det er kun e-post og web-oppslag til (og fra) andre aktører i helsenettet som kjøres over grensesnittet mot NHN. Kommunikasjon over dette grensesnittet går kun til og fra gradert/sikker sone i kommunens nett.

2.1.3 Endringer og nye programmer

Kommunikasjonsprogramvare

Meldingsutvekslingsprogrammet Well Communicator ble installert for å gi helsearbeiderne mulighet til å kommunisere med pasientenes tilsynslege eller fastlege ved å sende elektroniske meldinger. Det samme programmet gir brukerne mulighet til å sende sårmeldinger med bilde-vedlegg til hudavdelingen på UNN for å få råd og veiledning til å behandle sår hos pasientene. Sykehjemmene fikk mulighet til å motta elektroniske epikriser, polikliniske notat, labsvar og sykepleierdokumentasjon direkte fra alle avdelinger på UNN. Hjemmetjenesten fikk mulighet til å motta elektroniske epikriser, polikliniske notat og sykepleierdokumentasjon direkte fra alle avdelinger på UNN.

Well Communicator inneholder følgende funksjonalitet for å ivareta sikkerheten:

- Det er kun mulig å sende meldinger til forhåndsgodkjente mottakere
- Alle mottakere må legges eksplisitt inn i programmet, med tilhørende krypteringsnøkkel
- Alle meldinger blir kryptert før de blir sendt, for å hindre at uvedkommende skulle kunne lese meldingene som overføres

Well Communicator utveksler helseinformasjon gjennom meldingsbasert (asynkron) kommunikasjon. Kommunikasjonen skjer gjennom bruk av protokollene SMTP (meldinger ut) og POP (meldinger inn), og er et eksempel på bruk av "postkassemodellen", der meldinger blir hentet inn i sikker sone fra en postkasse. Bruk av "postkassemodellen" er med på å øke sikkerheten fordi all kontakt fra sikker sone og ut til omverdenen blir initiert innenfra og ut. I Tromsø kommunes brannmur var det kun åpnet for POP- og SMTP-trafikk fra den serveren Well Communicator kjørte på hos Tromsø kommune til EDI-serveren hos Norsk Helsenett.

Well Communicator er et kommunikasjonsprogram som ikke er ment å skulle brukes som et sluttbrukerprogram. Det er en forutsetning at fagsystemene har en kommunikasjonsmodul som kommuniserer med Well Communicator. Brukernes håndtering av meldinger

bør ideelt sett være en integrert del av fagsystemene, mens Well Communicator skal ta seg av konvoluttering, adressering, kryptering, etc. av meldinger mellom fagsystemene. Tromsø kommune har foreløpig valgt å ikke gå til anskaffelse av en kommunikasjonsmodul til fagsystemet som skal gjøre det mulig å motta elektroniske meldinger (i epikriseformat) fra blant annet Well Communicator. Grunnen til dette er dels at den ikke var ferdig pilotert og dels at kommunikasjonsmodulen i fagsystemet ennå ikke har funksjonalitet for å sende ut meldinger, slik at Well Communicator måtte bli brukt parallelt som sluttbrukerapplikasjon likevel. Fordi Well Communicator ikke er ment som en sluttbrukerapplikasjon, var det nødvendig at leverandøren gjorde enkelte tillempninger i programvaren for at den skulle fungere som sluttbrukerapplikasjon i en så kompleks organisasjon som pleie- og omsorgssektoren i en relativt stor kommune.

Well Communicator-løsningen består av to hovedkomponenter: en serverdel som sender og tar i mot meldinger, sørger for kryptering, adressering osv., og en klientdel som benyttes av brukerne. Kommunen har kun én installasjon av Well Communicator for hele pleie- og omsorgssektoren, men hver enhet i sektoren har sin egen konto som kun de har tilgang til.

Well Communicators brukergrensesnitt minner mye om et vanlig e-postprogram. En ting som skiller det fra et vanlig e-postprogram, er at meldinger går til kontoen til en avdeling og ikke til en spesiell bruker. Grunnen til dette er at ansatte på den samme avdelingen har behov for den samme informasjonen. Alle meldinger som er lest og merket som “behandlet” blir lagt i et arkiv. I arkivet har ansatte bare tilgang til meldinger fra sin avdeling. Dersom Well Communicator hadde vært integrert med fagsystemet, ville meldinger ikke blitt lagret her i kommunikasjonsprogrammet, men i fagsystemet, slik intensjonen er. På grunn av den manglende integrasjonen blir Well Communicator til en viss grad brukt som et journalsystem, noe det ikke er utviklet for. Tilgangsstyringsmekanismene i Well Communicator er ikke tilrettelagt med tanke på at programmet skal benyttes som et fagsystem med mange brukere. Det er kun tanken at administratorer og personell som har ansvar for avvikshåndtering av meldinger skal ha brukertilgang til Well Communicator.

Heretter vil vi benytte begrepet kommunikasjonsprogrammet eller kommunikasjonsløsningen når vi omtaler Well Communicator eller tilsvarende kommunikasjonsløsninger.

Tilgang til elektroniske prosedyrer

I SES@m-prosjektet ble det også laget en løsning hvor brukerne kunne få tilgang til elektroniske prosedyrer i Helse Nords prosedyrebank på Nordlandssykehuset. På desktop'en til brukerne ble det lagt et ikon de kan klikke på for å få direkte tilgang til prosedyrebanken. Dette gir personell i pleie- og omsorgssektoren enkel og rask tilgang til oppdaterte medisinske og behandlingsrelaterte prosedyrer som et ledd i kvalitetssikringen av pasientbehandlingen. Tilgangen var webbasert og utgjorde ikke en sikkerhetsmessig trussel for kommunen i og med at det kun var mulig å initiere trafikken (http på port 80) fra innsiden av kommunens nett mot Nordlandssykehuset via Norsk Helsenett.

2.1.4 Mobil tilgang

Sykepleiere i hjemmetjenesten i Tromsø kommune fikk, som en del av SES@m-prosjektet, bærbare datamaskiner som de kan bruke for å koble seg opp mot kommunens sikre sone via mobilnettet og Internett. Ved bruk av et innstikkskort fra Telenor eller NetCom i den bærbare datamaskinen, etableres det mobil tilgang til kommunens internettside for pålogging til det interne nettet i kommunen. Via tjenesten kan brukerne få tilgang til fagapplikasjoner med pasientopplysninger, som om de logget seg på fra hjemmetjenestens sonekontor.

Det ble benyttet en VPN-løsning for å gi helsepersonellet tilgang til kommunens interne nett og fagapplikasjoner. Hver enkelt bruker ble utstyrt med en kodegenerator med engangskoder eller et USB-token som plugges inn i den bærbare datamaskinen, og som gjør at brukeren kan autentiseres og gis tilgang på en sikker måte.

Ved hjelp av terminalserverløsningen som kommunen benytter kunne så brukerne gis tilgang til alle fagapplikasjonene de trenger på samme måte som om de satt ved lokale datamaskiner i kommunens eget nettverk. De mobile datamaskinene var konfigurert slik at det ikke skulle være mulig for brukerne å lagre pasientdata lokalt på datamaskinen

2.2 Viktigste trusler

2.2.1 Passordhåndtering

Håndteringen av brukernavn og passord innebærer mange potensielle svakheter. Noe av årsaken skyldes at brukerne må benytte flere sett med brukernavn og passord for å få tilgang til fagsystemene. Typisk krever noen systemer at passord byttes til faste tider (ofte ulikt for hvert system), noe som gjør det vanskelig for en IT-avdeling å lage brukervennlige rutiner for passordskifte. Det er også for liten bevissthet i sektoren knyttet til det å lage gode passord og å holde passordene hemmelig.

Det å måtte forholde seg til flere ulike passord, med ulike krav til kompleksitet og varierende krav til bytte av passord, har konsekvenser for sikkerheten på ulike måter. Et krav om å holde rede på mange og kompliserte passord medfører at brukeren må skrive ned passordene for å kunne benytte systemene, med tilhørende risiko for at disse kan komme på avveie. Uforholdsmessig kompliserte prosedyrer medfører også at brukerne søker etter veier å omgå systemet, for eksempel ved å dele på innloggingssesjoner framfor å logge ut og inn på nytt når en ny bruker må benytte systemet.

I sluttfasen av prosjektet arbeider Tromsø kommune videre med disse utfordringene for å finne tilfredsstillende løsninger. En mulighet som vurderes er å kunne benytte RSA-tokenet som benyttes mot VPN-løsningen også for pålogging til nettverket/terminalserverløsningen, noe som vil forenkle prosessen noe (se beskrivelse av løsningen i kap 4). Erfaringene fra SES@m Tromsø-prosjektet innebærer at dette er en problemstilling det må jobbes videre med før slike løsninger kan tas i bruk i stor skala.

2.2.2 Integrasjon av kommunikasjon i fagsystemet

En rekke av truslene som ble avdekket i vurderingen av risiko knyttet til bruken av løsningene i SES@m Tromsø-prosjektet relaterer seg til at kommunikasjonsløsningen er løsrevet fra de administrative systemene og fagsystemene som helsepersonellet benytter seg av. Pasientinformasjonen som kom inn til sykehjemmet eller hjemmetjenesten elektronisk ble

derfor i de fleste tilfeller skrevet ut fra kommunikasjonsprogrammet og lagret i papirjournalen.

Manglende integrasjon mellom kommunikasjonsprogrammet og fagsystemet er årsaken til flere av truslene med høyt eller middels risikonivå som ble avdekket i risikovurderingen. Dette er trusler som at epikriser og polikliniske notat sendes til feil enhet, at det kan ta lang tid før feilsendte epikriser og labsvar oppdages og at tilgang til meldinger angående "gamle" pasienter i kommunikasjonsprogrammet ikke blir fjernet. Disse truslene ble av brukergruppen vurdert å ha høy eller middels risiko, og illustrerer at dagens løsning med kommunikasjon via separat kommunikasjonsløsning allerede presser grensene for det akseptable. Hvis løsningene skal utbres til flere enheter og grupper i kommunen anbefales det derfor på det sterkeste at kommunen jobber for å få til løsninger som gjør at kommunikasjonen integreres i helsepersonellets fagsystemer.

En viktig grunn til at kommunikasjonsløsninger per i dag ofte må kjøres separat fra fagsystemene, er at leverandørene av fagsystemene ikke har implementert de standardiserte meldingstypene for helsesektoren som er utarbeidet av KITH, f.eks. PLO-meldingen. En annen grunn kan være at fagsystemene mangler en fullgod kommunikasjonsmodul som både håndterer innkommende og utgående meldinger. Manglende bruk av moduler for pleieplan og daglig rapportering i fagsystemene kan også være en medvirkende årsak til at kommunen ikke strekker seg maksimalt for å få til integrasjon mot kommunikasjonsløsningen. Så lenge den daglige rapporteringen i sektoren gjøres i papirjournal, vil det likevel være nødvendig å skrive ut viktige meldinger som kommer elektronisk, for å få en mest mulig samlet dokumentasjon.

Tilgangsstyring til informasjonen som er lagret i kommunikasjonsprogrammet er lagt opp slik at den enheten som har lagt inn informasjon/meldinger om en pasient er den enheten som eier informasjonen og skal ha tilgang til den. Dette gjør at enheten får tilgang til informasjonen også etter at pasienten er overført til en annen enhet, mens den nye enheten pasienten er overført til ikke får tilgang til gamle meldinger. Dette kan være en ulempe for den videre oppfølgingen av pasienten. På den annen side er det slik det fungerer i dag når hver enhet har sin egen papirjournal. Det kan dessuten tenkes at den nye enheten i henhold til helsepersonelloven § 45 må be om å få utlevert opplysninger fra den gamle enheten dersom det er behov for tilgang til denne informasjonen, i stedet for å hente ut informasjonen selv. Hvorvidt det er nødvendig å be om å få utlevert informasjon eller om informasjonen kan hentes ut av den som mener å ha behov for den, kommer an på om personellet på den nye enheten anses som samarbeidende eller annet helsepersonell. Se avsnitt om juridiske vurderinger i kapittel 5.4.1. Vi antar at personell på den nye enheten som oftest er å betrakte som samarbeidende personell. Dersom kommunikasjonsprogrammet og journalsystemet hadde vært integrert, kunne alle meldinger automatisk videresendes inn i journalsystemet og bli tilgjengelig for den som ut fra tjenestelig behov skal ha tilgang til journalen. Mens et elektronisk pasientjournalsystem har muligheter for fleksibel tilgangsstyring – hvor tilgang gis til brukere ved behov, i gitte tidsperioder hvor pasienten er aktiv osv – blir meldinger i kommunikasjonsprogrammet lagret i mappene til den avdelingen som sendte eller mottok meldingene (og ikke på den enkelte pasient), og kan dermed bli tilgjengelig for den aktuelle avdelingen i lengre tid enn nødvendig for behandlingen av pasienten.

Dette viser at det er et stort behov for å integrere kommunikasjonsløsningene med fagsystemene. Hovedfordelene med å integrere kommunikasjonen med fagsystemet er å:

- Sikre at alle meldinger dokumenteres i fagsystemet
- Unngå manuell overføring av opplysninger med fare for feilføringer
- Sikre at meldinger vedrørende pasient som ikke er registrert i systemet kan avvises
- Sørge for at styring av tilgang til informasjonen håndteres i fagsystemet og ikke i kommunikasjonsystemet.

2.2.3 Enklere sikker tilgang fra mobile klienter

I SES@m Tromsø-prosjektet er det lagt ned mye arbeid for å komme fram til sikre løsninger for å gi helsepersonell tilgang til fagsystemer og kommunikasjonsløsning fra mobile klienter, og vi har høstet mye erfaring om utfordringene rundt dette. I løpet av prosjektperioden er løsningen for autentisering av brukerne utviklet og endret mye for å gjøre den sikker, og samtidig brukervennlig. Mens man i henhold til risikovurderingene i stor grad har lyktes med å gjøre løsningene sikre, har man kommet kortere med å gjøre løsningene brukervennlige. Påloggingsprosedyren har ennå uforholdsmessig mange steg som må gjennomføres i til dels riktig rekkefølge.

Den kompliserte prosedyren som må gjennomføres for å få tilgang til kommunens nett og systemer medfører at grensen for å ta i bruk systemet for den enkelte helsearbeider heves. Årsaken til dette er både at prosedyrene er kompliserte og avskrekkende for ukyndige brukere, men også at prosessene tar for lang tid å gjennomføre i en stressende arbeidsdag. Dette medfører at løsningene ikke benyttes i så stor grad som ønskelig og nytteverdien av dem derfor reduseres tilsvarende. Det er sannsynligvis nattjenesten som opplever den lange påloggingstiden som mest problematisk, bl.a. fordi de får alarmer hvor det haster med å komme seg ut til pasienten. Den mobile tilgangen til fagsystemet gir kun informasjon om hvor pasienten bor, hvilke tjenester pasienten mottar, hvor nøkkel til huset finnes og om hvilket hjemmetjenestekontor som har informasjon om pasientens tilstand, medikamentbruk, diagnoser, etc. Dersom fagsystemet hadde vært oppdatert med opplysninger om diagnose, medikamentbruk, og lignende, hadde sannsynligvis nytteverdien av den mobile tilgangen vært så stor at sykepleierne i større grad ville benyttet den på tross av at det tar uforholdsmessig lang tid å logge seg på. Paradoksalt nok opplever likevel enkelte mobile brukere i distriktene at det er mer effektivt å få tilgang til kommunens IT-løsning via den mobile løsningen framfor via den stasjonære løsningen.

Hovedårsaken til de kompliserte påloggingsprosedyrene ligger i manglende integrasjon av autentiseringsløsninger på tvers av ulike IT-systemer, og er et generelt problem for alle løsninger av denne typen. For å få tilgang til fagapplikasjoner må brukeren autentisere seg overfor en rekke ressurser. Autentisering må foretas først mot selve datamaskinen, deretter mot kommunens brannmur og VPN-løsning, deretter mot terminalserverløsningen for å få tilgang til applikasjonene, og til slutt mot den enkelte fagapplikasjon. Hver av disse har egne og til dels ikke-integrerte systemer for å håndtere tilgangsstyring og autentisering av brukeren. Bedre integrering av autentiseringsløsninger kan gi sikre påloggingsmekanismer som samtidig ivaretar brukervennlighet.

3. Tilkobling til helsenettet og nye tjenester

Innholdet i dette kapittelet baserer seg i all hovedsak på resultatene fra risikovurderingen av tekniske løsninger i SES@m Tromsø-prosjektet. Fokus for denne risikovurderingen var endringer i trusselbildet for Tromsø kommunes nett og systemer som følge av installasjon av kommunikasjonsløsning i sikker sone, med kommunikasjon til eksternt nett.

I løpet av SES@m Tromsø-prosjektet åpnet Tromsø kommune for elektronisk kommunikasjon av helseopplysninger med andre helsevirksomheter. For å muliggjøre dette ble sikker sone i kommunens interne nett knyttet til Norsk Helsenett, og det ble installert en kommunikasjonsløsning for å utveksle meldinger over denne infrastrukturen. Risikovurderingen så på hvilke trusler som oppsto pga. denne endringen i kommunens infrastruktur.

De viktigste endringene ift. teknisk infrastruktur var:

- Tilkobling til eksternt nett (NHN) fra sikker sone
- Bruk av kommunikasjonsprogram for elektronisk kommunikasjon av sensitive data ut av kommunens nett

Vurderingene rundt innføringen av den mobile løsningen ble gjort i en egen risikovurdering. Resultatene fra denne er beskrevet i kapittel 4.

3.1 Teknisk infrastruktur og tilkobling til helsenettet

Kommunikasjonen fra Tromsø kommune til UNN og fast-/tilsynslegene går over kommunens tilknytning til Norsk Helsenett over fiberringen i Tromsø by. Legekontorer er koblet opp til NHN på samme måte som Tromsø kommune. Det er kun e-post og web-oppslag til (og fra) andre aktører i helsenettet som kjøres over kommunens grensesnitt mot NHN. Alle meldinger som sendes blir kryptert enkeltvis, i tillegg til krypteringen av selve VPN-forbindelsen mellom helsenettet og kommunens nett.

Internt var Tromsø kommunes nettverk bygd opp etter modell av Datatilsynets veiledning for kommuner, med sikker og åpen sone. All behandling av sensitive personopplysninger foregår i sikker sone. Se Figur 1. (side 14-15)

For å hindre lagring av sensitive data lokalt på de enkelte datamaskinene, benytter kommunen seg av en terminalserverløsning. Dette betyr at all prosessering av data skjer i en Citrix Metaframe-farm sentralt i Tromsø kommunes nettverk og at kun skjermbilder, tastatur- og musesignaler blir overført mellom klient-maskinen (den lokale datamaskinen) og Citrix Metaframe-farmen via en kryptert tunnel. Dette betyr en økt sikkerhet fordi ingen sensitive data blir lagret på klient-maskinen og all mulighet for klipp-og-lim, etc. mellom Citrix Metaframe sesjonen og klient-maskinen er deaktivert. Dersom uvedkommende skulle få tilgang til datamaskinene, vil de ikke finne pasientsensitive opplysninger på selve datamaskinene.

3.2 Elektronisk kommunikasjon

Kommunikasjonsprogrammet som ble benyttet for elektronisk kommunikasjon ut av sikker sone i kommunens nett er et meldingsbasert kommunikasjonsprogram. Det er spesielt utviklet for å transportere helserelaterte EDI-meldinger på en sikker måte mellom forskjellige enheter i helsesektoren. Man kan også legge ved digitale bilder, film, lydfiler eller andre typer vedlegg til meldingene. Det er kun mulig å sende meldinger til forhåndsdefinerte mottakere som er lagt inn i mottakerlista i kommunikasjonsprogrammet, med tilhørende krypteringsnøkkel. Det er ikke mulig å sende ukrypterte meldinger fra kommunikasjonsprogrammet.

Den samme kommunikasjonsprogramvaren som ble benyttet i Tromsø kommune var allerede i bruk på UNN og hos noen av legekantorene som er med i prosjektet ved prosjektstart.

Kommunikasjonsløsningen slik den er installert i Tromsø kommune vil være avhengig av tre ulike servere: En e-postserver i Norsk Helsenett, en server med kommunikasjonsprogrammet og tilhørende database og en Citrix Terminalserver i kommunens nett. E-postserveren fungerer som postkontor. Kommunikasjonsprogrammet sender med jevne mellomrom forespørsler om nye meldinger til e-postserveren, og laster ned de nye meldingene. Dette gjør at det er mulig å sperre for direkte kommunikasjon mot kommunikasjonsserveren fra eksterne nett.

Kommunikasjonsprogrammet lagrer mottatte meldinger i en database (enten lokalt som fil på serveren med kommunikasjonsprogrammet eller på en databaseserver), og kommuniserer med klientprogramvaren for å vise fram mottatte meldinger til brukeren.

3.3 Viktigste trusler

3.3.1 *Trusler med høyt risikonivå*

Risikovurderingene av de tekniske løsningene avdekket to trusler som bør trekkes fram som viktige å ta høyde for:

Manglende sikring av server med kommunikasjonsprogramvare

Serveren som kommunikasjonsprogrammet, inkludert meldingsdatabasen, ble installert på, var en såkalt "prosjektserver". Ved utprøving av nye løsninger, benyttes ofte en ikke-permanent teknisk løsning som gjerne kjører litt på siden av den ordinære maskinparken. Dette kan blant annet innebære at løsningen ikke omfattes av den rutinemessige backupordningen, og at backup kjøres med lavere hyppighet enn for andre deler av systemet med tilsvarende kritiske applikasjoner og databaser. Det vil også ofte være manglende redundans i løsninger som ikke har fått en permanent status. Ved et totalhavari av harddisken på en slik server, vil høyst sannsynlig data som er registrert siden forrige backup ble tatt, gå tapt. Ved overgang fra prosjektstatus til en mer permanent status for slike servere, er det lett å glemme eller ignorere den manglende sikkerheten, slik at risikonivået blir høyere enn akseptabelt for slike løsninger. Vi anbefaler på det sterkeste at det sørges for tilfredsstillende sikkerhet også i innføringsfasen av nye løsninger. Dette er spesielt viktig når prosjektperioden strekker seg over lengre tid, slik at man har en

Andre nettverk



Bærbar PC - Mobil hjemmetjeneste

- Pålogging i Sikker sone gir tilgang til
 - => Unique Profil fra Sikker sone
 - => Well Communicator fra Sikker sone
 - => DocMap - Elektroniske prosedyrer

- Pålogging i Intern sone gir tilgang til
 - => E-post fra Intern sone
 - => Webleser fra Intern Sone
 - => Økonomi, administrasjon mm. fra Intern sone



UNN - Universitetssykehuset i Tromsø

- * Mottar og besvarer sårhenvisninger
- * Sender ut:
 - => Elektroniske labsvar, polikliniske notater og epikriser
 - => Elektroniske utskrivingsmelding fra sykepleier på UNN til sykepleier på sykehjem og i hjemmetjeneste
- * Formidler tilgang til elektronisk prosedyrer (DocMap)



Berørt legekontor

- * Tilbyr Spørsmål- og svartjeneste v.h.a WELL Communicator

VPN/brannmur



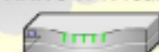
Mobilnett fra Netcom og Telenor
GPRS/EDGE/UMTS

Norsk Helsenett AS



NHN's e-posttjener for meldingsflyt i helsevesenet

NHN's VPN-router



Fiberring i Tromsø kommune

NHN's



Sykehjems- og hjemmetjenesteavdelinger

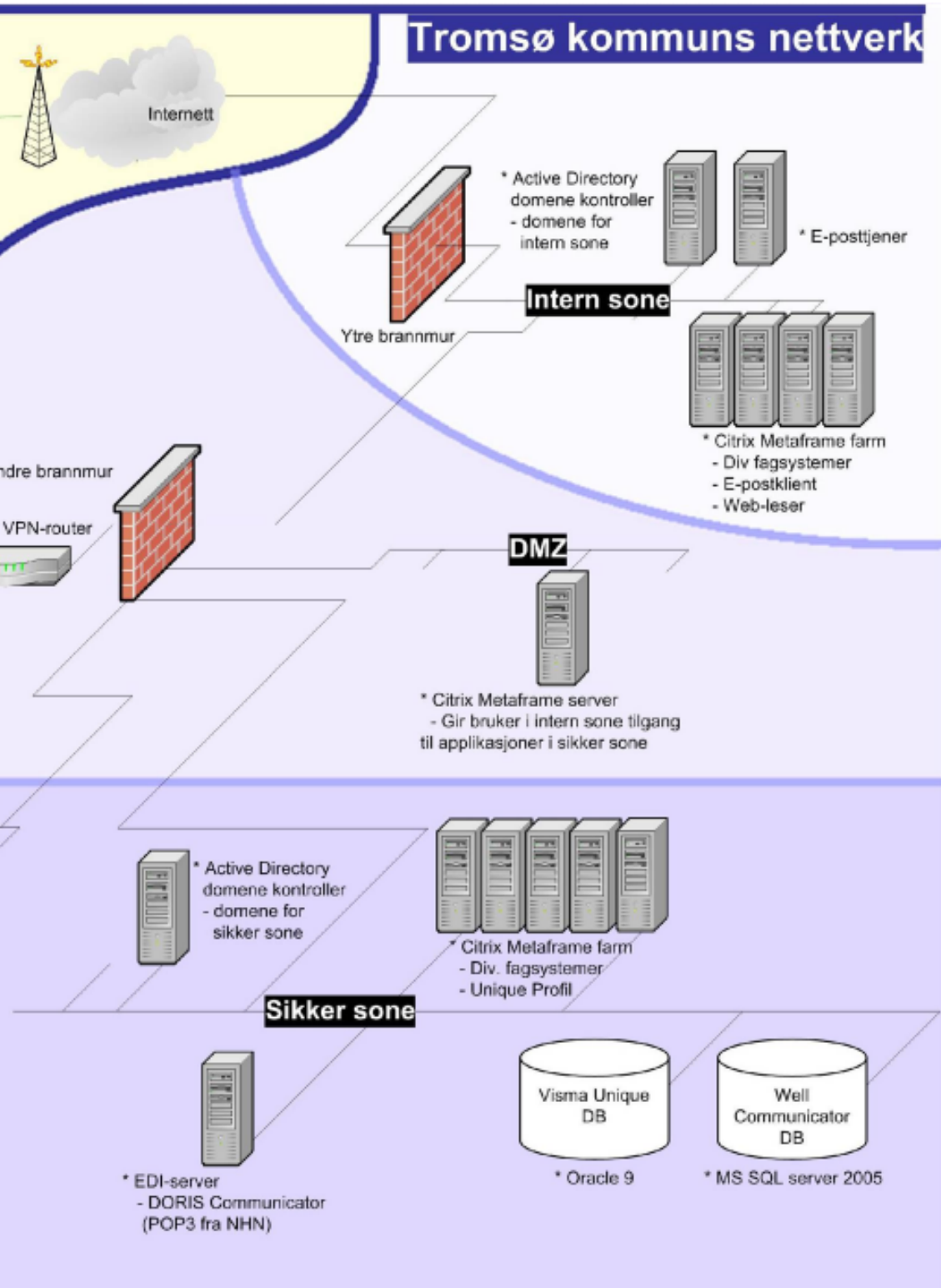


Stasjonære PC'er tilhørende i Sikker sone
* ICA klient

- Pålogging i Sikker sone gir tilgang til
 - => Unique Profil fra Sikker sone
 - => Well Communicator fra Sikker sone
 - => DocMap - Elektroniske prosedyrer
- Pålogging i Intern sone gir tilgang til
 - => E-post fra Intern sone
 - => Webleser fra Intern Sone
 - => Økonomi, administrasjon mm. fra Intern sone

Figur 1 Tilkobling til Norsk Helsenett og mobil tilkobling til kommunens sikre sone

Tromsø kommuns nettverk



tilnærmet normal driftssituasjon underveis i prosjektet, med lagring og behandling av til dels store datamengder.

Som en ekstra sikkerhet mot tap av meldinger som utveksles elektronisk, kan man vurdere å la meldingene i Exchange-innboksen i helsenettet bli liggende der et visst antall dager etter at de er pop-et fra kommunikasjonsprogramvaren. Tapte meldinger kan da hentes manuelt herfra etter et eventuelt havari av harddisken hvor kommunikasjonsprogramvaren er installert.

Bruk av ip-adresser fra private ip-ranger i helsenettet, og endring av ip-adresser

Norsk Helsenett har bl.a. benyttet private ip-adresser i sitt nett. Dette kan skape problemer ved tilknytning til helsenettet for virksomheter som bruker private ip-adresser i sitt lokale nett. For å kunne sende EDI-meldinger i NHN må en konto bestilles hos dem. Ved bestilling av nye EDI-kontoer (f.eks til bruk for et kommunikasjonsprogram i kommunen) tildeler NHN i noen tilfeller ip-adresser innenfor den private ip-rangen. Dersom disse ip-adressene er innenfor rangen av kommunens egne private ip-adresser vil det oppstå routing-problemer, og kommunen får en god del ekstraarbeid med manuelt vedlikehold av statiske routingtabeller. Det er slik sett svært uheldig at NHN benytter private ip-adresser i sitt nett.

I prosjektperioden opplevde vi også at kommunikasjonspartnere fikk ny ip-adresse uten at kommunen fikk beskjed om dette. Det medførte problemer med meldingsutvekslingen eller tilgangen til tjenester (tilgang til prosedyrebank). Slike årsaker til problemene kan være vanskelige å finne.

IT-avdelingen i Tromsø kommune opplevde dette som et vesentlig problem i SES@m-prosjektet. Dersom mange kommuner skal koble seg til helsenettet, antar vi at problemet vil øke ytterligere. Det vil da være mange flere aktører som kan oppleve å få endret ip-adresser. Ved manglende informasjon om dette til potensielle kommunikasjonspartnere, vil det kunne oppstå problemer med meldingsutvekslingen. Selv om informasjon om endring av ip-adresser blir gitt, vil det medføre ekstraarbeid for kommunene i og med at de må oppdatere statiske routingtabeller manuelt. Det er svært viktig at NHN endrer praksisen med å bruke ip-adresser fra private ip-ranger til sine kunder før et større antall av kommunene kobler seg opp mot helsenettet i nær framtid.

3.3.2 Trusler med lavt risikonivå

Flere av truslene med lav risiko knytter seg til at kommunikasjonsløsningen blir utilgjengelig pga. ulike systemtekniske svakheter i infrastrukturen hos kommunen eller helsenettet. Bruken av løsningen, hva angikk omfang og type meldinger som gikk, var i prosjektperioden ikke slik at kortere tids utilgjengelighet ble vurdert å ha stor konsekvens. Ved hastesaker følger helsepersonellet opp kommunikasjonen via andre kanaler, etterlyser svar osv., slik at dette til nå ikke er vurdert som en alvorlig trussel. Med en framtidig utvikling der volumet og typen meldinger som kommuniseres forandrer seg ved at det blir høyere trafikk eller at det overføres mer kritiske meldinger, bør dette følges opp med nye vurderinger og tiltak som sikrer at risikoen fremdeles er akseptabel. Dette kan være å innføre redundans i systemene, som for eksempel bruk av speilede databaseservere.

Spesielt i en innføringsfase, men også på mer permanent basis, vil det være viktig å ha

rutiner for avvikshåndtering som omfatter å sjekke om meldingsutvekslingen går som den skal. Ved etablering av kommunikasjon mot nye partnere kan det lett oppstå feil i registrering av mottakeradresser og krypteringsnøkler, med medfølgende problemer med meldingsutvekslingen. Noen på overordnet nivå (for eksempel IT-avdelingen i kommunen) bør regelmessig sjekke dette.

Ved innføring av nye tekniske løsninger og applikasjoner er det viktig at alle på IT-avdelingen får informasjon og opplæring om avhengigheter mellom systemene. Endring eller oppgradering av deler av systemet kan påvirke de andre delene av systemet. Det må lages gode rutiner for å sjekke at alle systemer fungerer som de skal etter oppgradering av systemene eller applikasjonene i kommunen.

4. Mobil løsning

4.1. Oppbygning og konfigurering

For å gi sykepleiere i distriktssonene og sykepleiere i nattjenesten i bysonen tilgang til kommunens nett og fagapplikasjoner, ble det benyttet bærbare datamaskiner med PCMCIA-innstikkskort i dette prosjektet. Det ble i alt plassert ut 9 stykk IBM X40 bærbare datamaskiner i Tromsø kommune. Disse datamaskinene gir tilgang til Internett via mobilnettet, og tilknytning via SSL VPN-forbindelse til kommunens nett. De bærbare datamaskinene kan også brukes stasjonært, da koblet til kommunens LAN ved hjelp av docking-stasjoner.

Det ble brukt forskjellig tilkobling og forskjellig typer mobilnett for de bærbare datamaskinene i distriktssoner og bysoner. Dekningskartene til teleoperatørene, opplysninger fra teleoperatørene om hvordan dekningsområdet kom til å bli seende ut, opplysninger om dekningen fra de lokale brukerne og kjøreturer der dekningen ble testet, ble lagt til grunn for hvilke operatører som ble valgt i hvilke områder. Resultatet ble at EDGE/GPRS-nettverk fra både Netcom og Telenor ble brukt, men i forskjellige soner.

Mobilkort brukt i distriktssoner

- Sierra Wireless AirCard® 775 EDGE PCMCIA-innstikkskort
- Sony Ericsson GC85 EDGE/GPRS PCMCIA-innstikkskort



Mobilkort brukt i bysonen

- HUAWEI E620 Mobile Connect UMTS/EDGE/GPRS PCMCIA-innstikkskort



Det var en uttalt forutsetning at det ikke skulle lagres noen sensitive opplysninger om pasienter lokalt på de bærbare datamaskinene i tilfelle de skulle komme på avveie. Det ble derfor naturlig å bruke en klient-tjener-løsning fra datamaskinene mot kommunens nett for tilgang til fagapplikasjoner med pasientinformasjon. Dette betyr at all prosessering av data skjer i en Citrix Metaframe-farm sentralt i Tromsø kommunes nettverk og bare skjermbilder, tastatur- og musesignaler blir overført mellom klient-maskinen og Citrix Metaframe-farmen via en kryptert tunnel. Dette gir en økt sikkerhet i og med at ingen sensitive data blir lagret på klient-maskinen og all mulighet for klipp-og-lim, etc. mellom Citrix Metaframe-sesjonen og klient-maskinen er deaktivert.

For å beskytte mot bl.a. ondsinnet programvare er det ønskelig å fjerne muligheten til å kommunisere mot andre nettstedene enn kommunens løsning for mobil tilgang. Den bærbare datamaskinen er tenkt som en løsning for å gi tilgang til applikasjoner i kommunens nett, og av sikkerhetsgrunner ønsker man derfor at den ikke skal kunne benyttes for eksempel til generell web-surfing over den mobile oppkoblingen. Dette kan løses på ulike måter. En måte er å bruke styringsmuligheter i Internet Explorer til å tillate at denne kun kan gå mot kommunens nettsted. Dette hindrer likevel ikke bruk av andre nettlesere til å koble seg opp mot Internett. Mer effektive tiltak vil kunne være å benytte lokale brannmurløsninger installert på hver bærbar datamaskin som kun tillater kommunikasjon mot

kommunens system. Det kan være en utfordring å få til slik sperring uten samtidig å skape problemer for klientoppkoblingen.

Med mobil tilgang til kommunikasjonsprogramvaren i kommunen kan man også sende sårbilder til hudavdelingen på UNN fra de bærbare datamaskinene. Det er i utgangspunktet ikke mulig å overføre data fra harddisken eller andre disker på eller tilknyttet den bærbare datamaskinen, til Tromsø kommune sitt nett via Citrix-forbindelsen (eller motsatt vei), f.eks. fra minnekortet på et digitalt kamera. For å få til overføring av sårbilder fra digitalt kamera eller kameraminnekort koblet til den bærbare datamaskinen via Citrix-Metaframe til serveren som kommunikasjonsprogramvaren er installert på (heretter kalt EDI-serveren), ble det benyttet et tilleggsprogram til Citrix Metaframe som heter Powerfuse. Powerfuse gjør det mulig å tillate overføring av bilder fra kamera eller kameraminnekort-leser som er tilkoblet den bærbare datamaskinen ved hjelp av USB-grensesnitt, til EDI-serveren. Brukeren vil dermed få tilgang til lokale disker på den bærbare datamaskinen når hun er inne i kommunikasjonsprogrammet og kan gå inn på kortleseren og hente frem nødvendige bilder. For at brukeren skal få tak i bildene må kameraet eller kortleser være koblet til USB-porten før brukeren logger seg inn i applikasjoner i Tromsø kommunes nett. Dette fordi Citrix laster ned tilgjengelige disker ved initiering av forbindelsen. Leverandøren av Powerfuse påstod at programmet skulle gjøre det mulig å styre på detaljert nivå hva brukeren skulle få lov til, ev. ikke få lov til, når man er koblet på en Citrix-sesjon i kommunens nett. Denne påstanden viste seg å være overdrevet. Det var kun mulig å styre at filoverføring bare skulle være mulig den ene veien og ikke motsatt vei.

4.1.1 Utfordringer ved flere brukere på bærbare datamaskiner

For å gjøre oppkoblingsprosessen fra de bærbare datamaskinene til fagapplikasjon så brukervennlig som mulig, var det nødvendig å gjøre en del konfigurering på hver enkelt datamaskin. Slike konfigureringer blir dessverre bare lagret i Windows-brukerens profil og er derfor bare gyldig for den brukeren de ble lagt inn for. Dette medførte at en slik konfigureringsjobb ville måtte gjøres for hver bruker som skulle ha tilgang til en bærbar datamaskin. For hver ny ansatt eller ny bruker ville det kreve at en tekniker tok en kjøretur ut i distriktssonen for å gjøre disse endringene. Fordi de mobile datamaskinene skulle deles av flere helsearbeidere pga skiftarbeid/turnusordning og at det ble for kostbart med en datamaskin per bruker, ble det lagt inn en felles Windows-bruker for hver avdeling med felles passord for oppstart av selve datamaskinen.

4.2 **Prosess for pålogging og autentisering**

En bruker som skal ha tilgang til de mobile tjenestene i kommunen, må igjennom en omfattende påloggingsprosess. Først må brukeren logge seg på lokal datamaskin (enten som seg selv eller som fellesbruker), deretter logge seg på VPN-løsningen og kommunens nettverk. Til slutt må brukeren autentisere seg mot fagapplikasjonen som skal benyttes. For å gjøre påloggingen sikker nok ble det benyttet to-faktor autentisering, dvs. en kombinasjon av noe man vet (f.eks. passord) og noe man har (f.eks. en påloggingsenhet).

Påloggingsenhet

Alt helsepersonell som skal arbeide med de bærbare datamaskinene har fått utstedt en USB-penn kalt eToken fra Aladdin med et personlig sertifikat fra kommunen, eller en

kodegenerator fra RSA kalt RSA SecureID. Autentisering av brukere er basert på noe de vet (passord) og noe de har (sertifikat på eToken eller kode på RSA-kalkulator). Sertifikatet på eToken er kryptert og må dekrypteres ved at brukeren skriver inn sitt personlige passord på datamaskinen som USB-penna er koblet til, for at brukeren skal bli autentisert mot kommunens autentiseringsserver. RSA SecureID er en kodegenerator som genererer en 6-sifret engangskode som vises i et lite display på enheten. Denne koden må brukeren oppgi ved innlogging, i tillegg til personlig brukernavn og passord. RSA SecureID genererer ny kode hvert minutt. Ved innlogging genererer kommunens autentiseringsserver den samme koden (ulike koder for de ulike brukerne). Disse kodene blir sjekket mot hverandre for å autentisere brukeren.

Pålogging på mobil datamaskin

For å få startet datamaskinen må brukeren oppgi et avdelingsspesifikt brukernavn og passord. Dette gir kun tilgang til selve datamaskinen, hvor det ikke skal ligge pasientopplysninger. Denne påloggingen til selve datamaskinen utgjør en ekstra sikkerhet, i og med at uvedkommende ikke uten videre kan starte datamaskinen og nyttiggjøre seg den.

På desktop'en til disse datamaskinene er det kun tre ikoner som brukeren kan benytte: ett for å starte mobilkort-applikasjonen, ett for å opprette en Internettforbindelse til intern sone i kommunen og ett for å opprette en forbindelse til sikker sone i kommunen. Disse måtte aktiveres i riktig rekkefølge for å få satt opp forbindelse til fagapplikasjonene i kommunens nett. Se beskrivelse under.

Pålogging til intern sone i kommunens nett –

Tromsø kommune benytter fjernaksesløsningen Check Point SSL Network Extender (SSL-VPN) for oppkobling til kommunens interne nettverk fra Internett.

Brukeren får satt opp en forbindelse fra mobilkortet i den bærbar datamaskinen over mobilnettet til Internett ved å klikke på ”Koble til”-knappen i applikasjonen som tilhører mobilkortet.

– med eToken

Hvis brukeren er utstyrt med eToken på USB-penn, setter hun denne i den bærbare datamaskinen og klikker på den første av de to snarveiene til Internet Explorer som ligger på skrivebordet. I snarveien er det lagret en URL-adresse til Tromsø kommune sin SSL Network Extender. Internet Explorer tar kontakt og brukeren får opp et vindu hvor hun blir bedt om å velge sitt sertifikat fra en liste. Denne lista inneholder sertifikatene til alle eToken-brukere som har vært inne på den bærbare datamaskinen. Brukeren velger sitt sertifikat og blir spurt om å skrive inn sitt personlige passord. Skriver brukeren inn riktig passord, vil eTokenet bli dekryptert og en SSL-forbindelse blir satt opp til Tromsø kommunes ytre brannmur. Hvis sertifikatet på eTokenet blir gjenkjent og funnet gyldig, gir Tromsø kommunes SSL Network Extender brukeren tilgang til intern sone via en kryptert VPN-tunnel over Internett. Den bærbare datamaskinen starter samtidig nedlasting av en ActiveX-kontroll (maskinen må tillate mottak av activeX-komponenter og java-plug-ins). ActiveX-kontrollen sørger for at tcp-konnektivitet kan kjøres over SSL, i dette tilfellet ICA-tcp trafikk på port 1494, for å etablere forbindelse videre til sikker sone i kommunens nett (se forklaring lengre ned).

Når tilgang til kommunens nett er etablert, kan eTokenet fjernes fra USB-porten. Det anbefales at dette gjøres til en rutine, slik at eTokenet ikke blir glemt i datamaskinen når den forlates.

– med RSA SecureID

Hvis brukeren i stedet er utstyrt med kodegenerator fra RSA SecureID, foregår autentiseringen ved at hun klikker på den første av de to snarveiene til Internet Explorer som ligger på skrivebordet. I snarveien er det lagret en URL-adresse til Tromsø kommune sin SSL Network Extender. Internet Explorer tar kontakt og det lastes ned en autentiserings-applet til datamaskinen. Det presenteres et vindu for brukeren der hun må fylle inn brukernavn og personlig 4-sifret PIN-kode sammen med en 6-sifret kode fra kodegeneratoren. Hvis kodene blir godkjent av kommunens autentiseringsserver, gir Tromsø kommunes SSL Network Extender brukeren tilgang til intern sone via en kryptert VPN-tunnel over Internett. Den bærbare datamaskinen starter samtidig nedlasting av en ActiveX-kontroll (maskinen må tillate mottak av activeX-komponenter og java-plug-ins). ActiveX-kontrollen sørger for at tcp-konnektivitet kan kjøres over SSL, i dette tilfellet ICA-tcp trafikk på port 1494, for å etablere forbindelse videre til sikker sone i kommunens nett (se forklaring lengre ned).

Forbindelsen til kommunen er tidsstyrt og varer i 4 timer. Når disse 4 timene er utløpt, må man koble seg opp/logge seg på på nytt om man har behov for fortsatt tilgang.

Pålogging til sikker sone i kommunens nett

Er oppkoblingen til intern sone i kommunen et faktum, vil brukeren kunne klikke på det andre Internet Explorer ikonet, som gir aksess til den interne innloggingssiden i kommunens nett. Her brukes Citrix® MetaframeXP™ for å sikre ende-til-ende kryptering fra den bærbare datamaskinen til sikker sone (via intern sone). Det kjøres en Citrix klient lokalt på den bærbare datamaskinen, som setter opp en ICA-sesjon mot kommunens Metaframe-server (tjener). All prosessering skjer sentralt på Metaframe-server. Det medfører at den bærbare datamaskinen kun får tilsendt endringer i skjermbilde. Brukerens interaksjon med mus og tastatur sendes fra klient til tjener.

I Citrix-innloggingsbildet i Internet Explorer må brukeren fylle inn sitt eget brukernavn, passord og hvilket domene brukeren vil logge inn på. Blir brukeren autentisert, vil hun få tilgang til de fagapplikasjonene hun er autorisert for, f.eks. kommunikasjonsprogrammet og/eller fagsystemet. Disse applikasjonene blir presentert for brukeren som ikoner på nettsiden, akkurat som om de skulle ligge på et skrivebord.

Pålogging til fagapplikasjoner i kommunens sikre sone

For å få startet fagapplikasjonene som inneholder sensitiv informasjon, må brukeren gjennom ytterligere en innlogging med brukernavn og passord per applikasjon.

En bruker vil kunne ha sikker sone oppe i én sesjon (ett skjermbilde) og intern sone opp i en annen sesjon (et annet skjermbilde) på samme tid. All mulighet for klipp-og-lim, etc, mellom de ulike sesjonene er deaktivert.

4.3 Sikkerhetsfaktorer og sentrale trusler

4.3.1 Autentisering, passord, osv.

Tilkobling til kommunens nett fra de bærbare datamaskinene forutsetter at brukeren benytter en påloggingsenhet (USB-penn med eToken eller en RSA SecureID-kalkulator). Dersom brukeren glemmer å ta med sin påloggingsenhet på jobb, vil det kunne medføre at brukere forsøker å låne hverandres påloggingstoken og passord. Det blir da ut fra dette ikke mulig å se hvilken bruker som har logget seg på kommunens nett. Brukeren må imidlertid logge seg på med eget passord for å få tilgang til fagsystemene. Det blir dermed likevel mulig å se hvem som har vært inne i fagapplikasjonen og lest og/eller dokumentert informasjon om pasientene. IT-avdelingen vil kunne spore at det ikke er samsvar mellom brukeren som logget seg på nettet og brukeren som benyttet denne nettilgang for å få tilgang til fagsystemene. Systematisk opplæring av brukerne om hvilke regler som gjelder og hva konsekvensen av slike brudd på regelverket kan føre til er viktig ved innføring av slike løsninger. Etablerte rutiner for hva brukerne skal gjøre når de har glemt eller mistet påloggingstoken er også viktig å ha på plass, for eksempel hvem man skal kontakte for å gi beskjed når noe er mistet og hvem man skal kontakte for å få tilgang til nødvendige pasientopplysninger, for eksempel over telefon.

En annen mulig trussel er at eksterne personer eller helsepersonell som er uautorisert for tilgang til fagapplikasjoner logger seg opp mot kommunens nett fra egen datamaskin eller kommunens bærbare datamaskin ved hjelp av stjålet eller lånt eToken eller RSA SecureID og PIN. Dette gir tilgang til kommunens infrastruktur, men for å komme inn i fagapplikasjoner kreves det i tillegg godkjent brukernavn og passord. For å hindre dette, eller i alle fall redusere denne trusselen, bør det legges inn sjekk av datamaskinene som brukere kobler seg opp fra, for å sikre at det kun er mulig å logge seg på fra kommunens egne datamaskiner. Videre er det viktig å bevisstgjøre brukerne på å melde fra om tapt token og/eller tapt datamaskin umiddelbart, slik at disse kan bli sperret for tilgang til kommunens systemer. Brukerne bør også bevisstgjøres om at de ikke skal låne bort token, PIN-koder og RSA SecureID-kalkulator.

En relativt vanlig trussel er at brukernavn og passord kan være kjent blant kollegaene eller være oppskrevet og ligge lett tilgjengelig for kollegaer eller utenforstående. Dette har særlig sammenheng med det høye antall passord en bruker må ha oversikt over for å få tilgang til sine applikasjoner. For mobil tilgang kreves i tillegg eToken eller RSA SecureID med tilhørende PIN-kode for å få tilgang til kommunens nett. Slik sett kan bruk av bærbare datamaskiner i kombinasjon med påloggingsenhet og PIN gjøre denne trusselen mindre enn ved bruk av stasjonære datamaskiner med kun passord. Det er uansett viktig at passordrutiner og oppfølgingen av disse er godt gjennomtenkt og implementert for å hindre at passord ikke er lett tilgjengelig. Kommunen bør også tilstrebe å ha påloggingsprosedyrer som ikke krever bruk av for mange ulike passord for hver bruker, for ofte bytte av passord, og bytte av passord til ulike tider for de ulike nett, systemer og applikasjoner.

I utgangspunktet skiller ikke VPN-løsningen mellom hvilke datamaskiner som benyttes for å logge på VPN-løsningen. Man kan i teorien benytte hvilken som helst datamaskin med internettilknytning sammen med kodegenerator fra RSA SecureID eller eToken fra

Aladdin for å koble seg opp mot kommunens nett. Skal man benytte eToken, må eToken-driveren og kommunens sertifikat være installert på datamaskinen. Man kan kun bruke et eToken eller en RSA SecureID som er registrert på en gitt bruker i kommunen. Man må også kjenne URL-adressen til kommunens påloggingside for å få logget seg på. Det kan anbefales å benytte løsninger som i tillegg kan sjekke hvilke datamaskiner som prøver å logge seg på.

4.3.2 Tap av mobilt utstyr

Bærbare datamaskiner er attraktive tyveriobjekter. Tap av bærbare datamaskiner, ev. med sensitive opplysninger, eller av kamera eller kamerakort med bilder av pasienter, utgjør således en trussel. Noen viktige tiltak ble identifisert i SES@m Tromsø-prosjektet: Datamaskinene bør merkes tydelig med kommunens navn, gjerne på lokket, og det bør gis rutinemessig opplæring av de ansatte med hensyn til hvordan datamaskinene, eToken/RSA SecureID og kameraene/kamerakortene bør oppbevares. Det er fort gjort å glemme igjen datamaskinen i bilen når den forlates, for eksempel for å ta en tur innom butikken. Å fjerne mulighetene, så langt det lar seg gjøre, for at brukerne kan lagre sensitive opplysninger på de bærbare datamaskinene er derfor viktig. Det er også mulig å lage en rutine for sletting av bilder, ev. et script som superbruker kan kjøre rutinemessig og som sletter alle bilder på den bærbare datamaskinen.

Det er en større trussel at bærbare datamaskiner som er pålogget fagsystemer kan bli stjålet, enn at stasjonære datamaskiner inne på sonekontorene til hjemmetjenesten blir stjålet. Med mindre brukeren alltid logger seg ut av fagsystemene når hun er ferdig med å lese og/eller dokumentere informasjon om en pasient, kan en pålogget datamaskin bli stjålet, f. eks. fra bil. Det vil være naturlig å benytte en passordbeskyttet skjermsparer på de bærbare datamaskinene, som slår seg inn etter en gitt periode. Men dersom datamaskinen stjeles før skjermspareren har slått inn, kan den som stjeler datamaskinen kunne få tilgang til fagsystemene med samme rettigheter som den påloggede brukeren hadde. Dette krever imidlertid at datamaskin-lokket åpnes og at den som stjeler datamaskinen forsøker å tilegne seg eller endre informasjon umiddelbart. Ved eventuell omstart av datamaskinen vil det være nødvendig å oppgi brukernavn og passord og i tillegg benytte eToken eller engangskode fra RSA SecureID. Det bør derfor etableres rutiner for situasjoner hvor datamaskinen blir stjålet, som omfatter hvem som skal varsles og hva som skal gjøres (sperre evt token, sjekke om det har vært aktivitet fra denne brukeren i fagsystemene i perioden etter at datamaskinen ble stjålet, og lignende).

USB-penna med eToken og RSA SecureID-kalkulator bør ikke merkes med eierens brukernavn, men heller med eierens navn. Dette vil gjøre det vanskeligere for uvedkommende å nyttiggjøre seg påloggingsenhetene hvis de mistes eller blir liggende tilgjengelig for andre, samtidig som det blir mulig for eieren å kjenne igjen sin påloggingsenhet.

4.3.3 Hacking og ondsinnet kode

Det vil alltid være en trussel at ondsinnet kode kan komme inn i kommunens nett via den bærbare datamaskinen. Programvare som beskytter mot både virus, ormer, spyware og annen potensielt skadelig programvare bør installeres på datamaskinen og oppdateres jevnlig. Om nødvendig må det kreves at de bærbare datamaskinene kobles til fastnettet på hjemmetjenestekontorene jevnlig for oppdatering av sikkerhetskritisk programvare.

Det bør være mulig å spore når de ulike datamaskinene har blitt oppdatert, slik at datamaskiner som har gamle versjoner av sikkerhetsoppdateringer kan bli innkalt for oppdatering. Man bør også søke å finne løsninger som ikke krever at brukerne må være lokale administratorer på datamaskinen, for å sperre muligheten for å legge inn programvare.

Hacking av datamaskinen fra Internett er en potensiell trussel så lenge brukeren er avhengig av å koble seg opp mot Internett for å få tilgang til VPN-løsningen. Det er derfor ønskelig å begrense mulighetene for konfigurasjonsendringer og for å installere ny programvare (bl.a. for å hindre ondsinnet kode i å installere seg på systemet). Man bør derfor finne løsninger som ikke krever at brukerne må være lokale administratorer på datamaskinen for å få koblet seg opp mot kommunens nett. Det bør også være effektive funksjoner for å hindre installasjon av andre nettlesere enn Internet Explorer. En mulighet er å ta i bruk et program som tilbakestiller brukerkonfigurasjonen på datamaskinen til opprinnelig konfigurasjon hver gang datamaskinen startes.

4.3.4 Manglende tilgang

Teknologien som benyttes for å gi mobil tilgang er avhengig av en rekke løsninger som må fungere. Problemer med oppkobling til kommunens nett pga problemer med servere, VPN-tilkoblingen, planlagt nedetid for systemene, gjenglemt eller tapt eToken, RSA SecureID eller PIN eller problemer i mobilnettet vil medføre at brukerne ikke får tilgang til sine fagapplikasjoner. Det bør opprettes manuelle rutiner for tilgang til informasjon og dokumentasjon når den mobile tilgangen svikter.

Løsningen som ble implementert i SES@m Tromsø-prosjektet har sine begrensninger, bl.a. den lange tiden det tok fra bærbar datamaskin ble slått på til brukeren var logget på kommunens sikre sone og klar til å arbeide. Tromsø kommunes infrastruktur og sikkerhetskrav fra Datatilsynet la premisser for hvilke valg som ble fortatt i prosjektet når det gjaldt autentiseringsløsninger. Dette medførte at oppkoblingstiden fra brukeren slo på maskinen til hun/han hadde tilgang til fagapplikasjoner med sensitive opplysninger var ca. 7-8 min. Hvis kontakten mellom bærbar datamaskin og Tromsø kommunes servere ble brutt som følge av for eksempel dårlig mobildekning, måtte innloggingsprosessen startes fra begynnelsen igjen.

4.3.5 Avlytting av mobil forbindelse

Vi vurderte også trusselen om avlytting av den mobile forbindelsen via mobilnettet eller Internet. VPN-løsningen mellom den bærbare datamaskinen og den ytre brannmuren i kommunens nett er kryptert og støtter AES og trippel DES. I tillegg benyttes det en Citrix-Metaframe-forbindelse som krypterer forbindelsen ende-til-ende mellom datamaskinen og den indre brannmuren i kommunen. Vi antar derfor at dette i praksis ikke er en realistisk trussel.

5. Brukeraspekter

Svært mange av truslene vi avdekket i risikovurderingene i SES@m-prosjektet var brukerrelaterte. Disse hadde også høyest risikonivå. Vi vurderte spesielt trusler relatert til uautorisert tilgang og manglende tilgang til pasientopplysninger. Under gir vi en oversikt over sikkerhetsmessige utfordringer fra brukersiden.

5.1 Passord

Håndteringen av brukernavn og passord innebærer mange potensielle svakheter. Noe av årsaken skyldes at brukerne må benytte flere sett med brukernavn og passord for å få tilgang til fagsystemene. Det er også for liten bevissthet i sektoren knyttet til det å lage gode passord og å holde passordene hemmelig. Ofte blir brukernavn og passord skrevet opp, eller de er enkle å gjette.

Mange brukere har samme brukernavn på nettdomenet og i fagsystemene, og velger i utgangspunktet også samme passord for alle systemene. Dette gjør at det er viktig for IT-avdelingen i kommunen å utstede ulike passord til brukerne ved første gangs tildeling av brukernavn og passord. Brukernavn er ofte enkle å gjette hvis man vet hva brukeren heter. Noen av systemene som benyttes krever at passord byttes til faste tider (ulikt for hvert system), noe som gjør det vanskelig for IT-avdelingene å lage brukervennlige rutiner for passordskifte.

Det bør aktiveres automatisk endring av passord ved første gangs pålogging til fagsystemene. Kommunikasjonsprogrammet som ble benyttet i SES@m-prosjektet krever aldri at passordet skal endres, men det er mulig å legge inn tvunget passordskifte til faste tider. Vi anbefaler at dette gjøres. Forenklede påloggingsprosedyrer (færre sett med brukernavn og passord for hver bruker) og opplæring i risikoen dersom passord kommer uvedkommende i hende, vil redusere risikoen for mange av truslene relatert til passordbruk. Opplæring i hvordan man kan lage gode passord som er lette å huske men vanskelig å gjette, vil også være et nyttig tiltak.

Misbruk av passord på avveie krever at en angriper har fysisk adgang til en maskin som er knyttet til sikker sone (gradert nett) i kommunens nett for å kunne få tilgang til fagapplikasjoner i sikker sone. For å kunne avdekke hvem som har logget seg på med ”stjålet” brukerID bør det spores hvilken datamaskin brukeren har logget seg på fra.

5.2 Utskrift

Det er en kjent problemstilling at utskrifter kan bli liggende på skrivere lett tilgjengelig for uvedkommende. I SES@m Tromsø-prosjektet har vi erfart ulike årsaker til at utskrifter kan bli liggende uforholdsmessig lenge på skriveren, med mulighet for at uvedkommende kan få tilgang til dem, eller at utskrifter kan komme på avveie.

Skrivere står ofte i korridorene på sykehjem eller i hjemmetjenestens lokaler. Selv om skrivere står på vaktrom, er de ofte uten tilsyn av ansatte, pårørende, pasienter eller andre derfor kan gå inn og lese.

Det er viktig å ha rutiner for at utskrifter hentes umiddelbart hvis skriver står i korridor eller på åpne vaktrom. Eventuelt bør man sørge for at skrivere står i umiddelbar nærhet av datamaskinen, og gjerne ha skriverrom som er avlåst.

Utskrift med pasientopplysninger kan også komme på avveie i kommunen. Hvis kommunen har mange skrivere som kan nås av mange brukere, kan utskriftene også havne helt andre steder enn der de skal. Det kan i en del tilfeller være vanskelig for brukeren å kontrollere om utskrift har kommet ut, og i tilfelle hvor.

Vår erfaring var at utskriftsfunksjonen ikke alltid fungerte etter hensikten. Noen ganger fungerte den tilsynelatende ikke i det hele tatt. Ved tekniske problemer med skrivers ble utskrifter liggende i kø til skriver eller system fungerte igjen, og ingen visste når utskriftene kom. Datamaskinene var satt opp til automatisk å velge nærmeste skriver, men dette fungerte ikke alltid etter hensikten. Hvis brukerne klikker på utskriftsikonet i verktøylinja for å få utskrift, legger de som oftest ikke merke til hvilken skriver utskriften sendes til.

Ved bruk av terminalserverløsning er det hensiktsmessig å bruke en utskriftsløsning hvor driverne til hver brukers skrivere ikke ligger på terminalserverne. De trenger kun å ligge på brukerens lokale maskin. Tromsø kommune brukte utskriftsløsningen ThinPrint. Med denne løsningen ligger det en enkelt ThinPrint-driver på terminalserverne. I tillegg til å gjøre terminalserverne stabile, gir denne løsningen også hver enkelt bruker mer kontroll over skriveren, siden det i praksis skrives ut til en lokal skriver. Dermed kommer alle skuffer og innstillinger på hver skriver opp, og det blir et ledd mindre å undersøke ved eventuelle utskriftsproblemer. Brukeren vil også få opp et bilde på skjermen av utskriften før den blir skrevet ut, slik at eventuelle feilutskrifter kan stoppes. Vår erfaring er imidlertid at konfigurasjonen av en slik løsning kan være en utfordring. Dersom man av kapasitets- og stabilitetshensyn har flere Citrix Metaframe-servere som brukerne kan bli knyttet opp mot når de logger seg på kommunens nett, er det viktig å sørge for at alle disse serverne er konfigurert rett med hensyn på hvilke brukere som skal ha tilgang til hvilke skrivere i ulike situasjoner. For eksempel anbefales det at når sykepleiere logger seg på nettet fra en mobil datamaskin via det mobile nettet, bør de ikke ha tilgang til skrivere i det hele tatt, da de sannsynligvis ikke befinner seg i nærheten av en skriver. Skal de ha tilgang til skrivere, må de koble seg opp via fastnettet på hjemmetjenestekontoret. Citrix Metaframe kan skille mellom hvilke mobile datamaskiner som er koblet opp via mobilnettet og hvilke som er koblet opp via fastnettet. Det er også viktig å sikre at brukerne har de nødvendige rettigheter for å kunne skrive ut på lokal skriver.

Det er viktig å ha rutiner for å teste utskrift fra programmene når de installeres, og å bevisstgjøre brukerne til å sjekke hvilken skriver utskriftsfunksjonen har valgt.

5.3 Dårlig eller manglende tilgjengelighet

Enkelte brukere sliter med foreldet utstyr og programvare og for dårlig linjekapasitet i nettet. Dette medfører bl.a. at meldinger leses seint, siden det tar for lang tid å logge seg på systemet. Noen av datamaskinene er veldig trege. Mange av brukerne har lite datakunnskap og vil ikke nødvendigvis forstå om problemene skyldes tekniske problemer,

kapasitetsproblemer i nettet eller at det bare tar lang tid å starte opp datamaskinen, og gir ofte opp påloggingsforsøket dersom det ikke går raskt nok. Løsningen på dette vil være å oppgradere utstyrsparken og nettinfrastrukturen.

Flere tekniske faktorer kan medføre at systemet ligger nede slik at brukere ikke får hentet ut pasientinformasjon. Dette skjer oftere for natttjenesten enn andre, bl.a. fordi planlagt nedetid for oppgradering av systemet oftest er på kvelds- eller nattetid. Så lenge man også har papir-journal, kan brukerne låse seg inn på sonekontoret og finne opplysninger der. Dette forutsetter at helsepersonellet vet hvilken sone pasienten tilhører (mest kritisk når det går alarmer). Ved overgang til kun elektronisk journal, vil problemet bli mye større. Tilgjengeligheten for natttjenesten bør derfor bedres, og planlagt nedetid på kveld og natt må koordineres med natttjenesten.

Kommunen har foreløpig ikke tatt i bruk pleieplan- og rapportmodulene i fagsystemet. Siden fagsystemet ikke brukes fullt ut blir informasjon, både når det gjelder diagnoser, adresse og pårørende, ikke oppdatert i en slik grad at den alltid er til å stole på. Disse opplysningene ligger stort sett bare i papir-journalen. Dette er særlig et problem for mobile brukere som ikke har tilgang til denne. Disse problemene forventes å bli mindre når kommunen tar i bruk pleieplan- og rapportmodulene i fagsystemet, forutsatt at fagsystemet og support da er tilgjengelig 24 timer i døgnet.

5.4 Organisatoriske aspekter

Selv om meldinger sendes fra eller går til avdelingens konto i kommunikasjonsprogramvaren og ikke en spesiell brukers konto, registreres det likevel hvilken bruker som har sendt meldingen eller som har lest og eventuelt (fulgt opp og) arkivert innkommende meldinger

Alle meldinger som er lest og avhuket som behandlet blir lagt i et arkiv. Både i innboksen og i arkivet har ansatte bare tilgang til meldinger tilhørende sin avdeling.

Distribuerte pasientopplysninger

Den versjonen av fagsystemet som Tromsø kommune benytter for pleie- og omsorgssektoren hadde ikke muligheter for å ta i mot elektroniske meldinger fra kommunikasjonsprogrammet, eller sende meldinger ut. Pasientinformasjonen som ble akkumulert i kommunikasjonsprogrammet var derfor ikke tilgjengelig fra fagsystemet. Dette førte til at pasientinformasjon som ble lagt inn i fagsystemet ble lagret i én database, og pasientinformasjon som ble kommunisert gjennom kommunikasjonsprogrammet ble lagret i en annen. Det totale bildet av en pasients helseopplysninger befant seg derfor på tre forskjellige steder: i kommunikasjonsløsningens database, i fagsystemets database og i papirjournalen. Opplysningene i de to databasene var komplementære. De fleste meldinger som kommer inn til sykehjemmet eller hjemmetjenesten via kommunikasjonsprogrammet blir skrevet ut og lagret i papirjournalen. De resterende blir kun liggende i arkivet i kommunikasjonsprogrammet.

Når det gjelder labsvar eller meldinger om medisinerings fra fastlege/tilsynslege, blir disse i noen tilfeller skrevet manuelt inn i kurvearket, uten at det tas utskrift av selve mel-

dingen. I og med at journalsystemet foreløpig ikke brukes til annet enn pasientadministrative oppgaver, og at papirjournalen fortsatt benyttes som journal, utgjør ikke dette noen stor trussel i dag. Når kommunen går over til kun å bruke elektronisk journalsystem (uten at meldingene i kommunikasjonsprogrammet blir integrert i fagsystemet/journalsystemet) vil imidlertid dette bli et større problem. Innholdet i meldinger i kommunikasjonsprogrammet vil da måtte skrives inn i journalsystemet, noe som vil kreve ekstra tid i en allerede travel hverdag og gå på bekostning av tiden som kunne vært brukt ute hos pasientene.

Dersom opplysninger skal overføres manuel mellom applikasjonene/systemene, gir dette mulighet for feil, både med tanke på kvalitet og om opplysningene blir knyttet til rett pasient.

Manglende integrasjon mellom kommunikasjonsprogrammet og fagsystemet (journalsystemet) er årsaken til en del av truslene med høyt eller middels risikonivå, bl.a. organisatoriske utfordringer knyttet til oppfølging av meldingene, som beskrevet nedenfor.

5.4.1 Oppfølging av meldinger (feilsendte og innkommende)

Feilsendinger med tekniske årsaker

I den versjonen av kommunikasjonsprogrammet som ble benyttet i prosjektet, var det slik at alle meldinger om en pasient som kom til kommunens pleie- og omsorgssektor ble sluset til kontoen (innboksen) til enheten der helsearbeideren som stod som ansvarlig bruker for pasienten i kommunikasjonsprogrammet, er ansatt. Dette skyldes at dette kommunikasjonsprogrammet konfigureres med en ansvarlig bruker for hver pasient første gang det sendes en elektronisk melding om pasienten. Den personen som legger pasienten inn i kommunikasjonsprogrammet blir registrert som ansvarlig bruker. Enheten der personen jobber vil motta meldingene som kommer om denne pasienten. Det at meldinger ble sluset til kontoen til enheten der den som stod som ansvarlig bruker for pasienten jobbet, skjedde uavhengig av hvem avsenderen hadde valgt som mottaker i kommunen og uavhengig av hvem som eventuelt hadde sendt en henvisning eller rekvisisjon som genererte denne svarmeldingen. Denne situasjonen kunne for eksempel oppstå hvis en pasient som mottok tjenester fra hjemmetjenesten fikk et korttidsopphold på sykehjem og sykehjemmet sendte en rekvisisjon til sykehuset eller laboratoriet. Svarmeldingen kom da til hjemmetjenestens konto i kommunikasjonsprogrammet og ikke til sykehjemets konto. Hjemmetjenesten måtte da manuelt endre ansvarlig bruker i kommunikasjonsprogrammet til ”ingen ansvarlig”, åpne meldingen og velge riktig enhet som ansvarlig for behandlingen av meldingen. Meldingen la seg da i riktig innboks.

En annen problemstilling knyttet til det at den som først legger inn pasienten i kommunikasjonsprogrammet blir satt som ansvarlig bruker for pasienten, er at hvis denne helsearbeideren overflyttes til en annen enhet i kommunen, vil nye meldinger om pasienten komme til den nye enheten helsearbeideren jobber på og ikke til den enheten pasienten tilhører.

I løpet av prosjektperioden gjorde leverandøren en rekke endringer i den utgaven av kommunikasjonsprogrammet som ble benyttet av kommunens pleie- og omsorgssektor. Endringene skulle bl.a. medføre at meldinger sluses til kontoen (innboksen) til meldin-

gens adressat uavhengig av hvilken enhet som er registrert som ansvarlig bruker for pasienten i kommunikasjonsprogrammet, slik at meldingene kommer til revirentens enhet og ikke til noen andre. SES@m Tromsø-prosjektet ble avsluttet før ny versjon med disse endringene ble levert, men en pilotversjon med noen av endringene ble testet av NST og fungerte tilsynelatende i tråd med hensikten.

Ved bruk av en kommunikasjonsløsning som ikke er integrert i journalsystemet er det viktig å tenke gjennom denne type problemstillinger, og sjekke med leverandøren(e) hvordan deres løsning håndterer disse tingene.

Framtidig integrering av elektroniske meldinger i journalsystemet vil imidlertid medføre at meldingene går inn i journalen til pasienten og blir tilgjengelig for de som ut fra tjenestelig behov skal ha tilgang til journalen, og ikke for noen andre. Dette burde være et viktig incentiv for å oppgradere journalsystemet med meldingskommunikasjon (mulighet for å motta og sende meldinger).

Feilsendinger med organisatoriske årsaker

Epikriser, labsvar, polikliniske notat og utskrivningsmeldinger sendes noen ganger til feil enhet. Sykehus har ofte unøyaktig informasjon om hvilken institusjon eller hjemmetjenesteenhet pasienten er tilknyttet. Pasienter, pårørende og andre kan i noen tilfeller gi unøyaktig informasjon om hvor pasienten hører hjemme (for eksempel Kroken sykehjem i stedet for Omsorgstjenesten Jadeveien, som tidligere lå under Kroken sykehjem). De ansatte på sykehuset har ikke alltid god nok oversikt over sykehjemmene eller hjemmetjenestesonene i kommunene. Feilsendinger medfører at det tar lengre tid før meldingen kommer til riktig mottaker. At sykehuset alltid ringer før utskrivning og gir beskjed til enheten om utskrivningen, reduserer konsekvensene knyttet til eventuell feilsending av utskrivningsmeldinger.

Når det benyttes en kommunikasjonsløsning hvor avsender må adressere meldingen til riktig enhet i kommunen, må kommunen gi tydelig informasjon til de sykehus og virksomheter (for eksempel legevakt) det er relevant å sende pasientene til, om hvordan pleie- og omsorgssektoren i kommunen er organisert, og hvordan epikriser, polikliniske notat, labsvar og utskrivningsmeldinger mm til kommunens enheter skal adresseres. Sykehusene på sin side bør gå gjennom sine rutiner og forbedre dem. Kommunene må etablere gode rutiner for oppfølging av feilsendte meldinger. Integrasjon av den elektroniske kommunikasjonen i fagsystemene for pleie- og omsorgssektoren vil redusere noe av problemet med feilsendte meldinger ved at meldinger kan gå til et felles mottak for kommunen og fordeles på basis av pasienttilhørighet. Dette vil også gjøre det lettere å oppdage meldinger som er feilsendt til kommunen.

Utfordringer ved oppfølging av feilsendte meldinger

Det kan i noen tilfeller ta lang tid før feilsendte epikriser, labsvar og lignende oppdages. Meldingene må leses i kommunikasjonsprogrammet fordi kommunikasjonen ikke er integrert i den elektroniske journalen på sykehjem eller i hjemmetjenesten. Ansatte på sykehjem har ikke oversikt over pasientene på andre avdelinger på samme sykehjem og ser derfor ikke at meldinger er feilsendt (de ulike avdelingene på samme sykehjem hadde felles brukerkonto i kommunikasjonsprogrammet). Epikriser kan bli liggende i kommuni-

kasjonsprogrammet uforholdsmessig lenge før det oppdages at de er feilsendt. I tillegg er det ikke nødvendigvis alle brukere som vet hvordan de skal returnere en feilsending. Det kan derfor gå en del tid før rette mottaker får epikrisen eller labsvaret. Ved meget kritiske meldinger forutsettes det at helsepersonellet på sykehuset følger opp med telefon.

Integrasjon av den elektroniske kommunikasjonen i fagsystemene for pleie- og omsorgssektoren vil redusere noe av problemet med feilsendte meldinger. Meldingene vil da komme rett inn i pasientens journal og være tilgjengelig for alle som har rettmessig tilgang til journalen. Ved integrering i journalsystemet må enhetene etablere rutiner for rutinemessig sjekk av innkommende meldinger.

Kommunen bør tilstrebe å ha superbrukere på hver avdeling der dette er hensiktsmessig. Disse bør ha gjennomgang av ikke-arkiverte meldinger som rutineoppgave.

Juridiske vurderinger knyttet til én felles journal for hele pleie- og omsorgssektoren i kommunen

I henhold til helselovgivningen, jmf. journalforskriften, skal virksomhet hvor det ytes helsehjelp opprette journalsystem med journalansvarlig. Sykehjem og hjemmetjenesten er eksempler på slike virksomheter. Hver kommune har én databehandlingsansvarlig, som bl.a. har ansvar for alle journalsystemene innen kommunens pleie- og omsorgssektor. Ved innføringen av elektronisk journal i pleie- og omsorgssektoren, kan man tenke seg at det opprettes én journal pr. pasient i dette journalsystemet. For å imøtekomme kravet om at kun de som har tjenestelig behov for tilgang til sensitive opplysninger får det, må tilgangsrettighetene styres slik at bare de som jobber på den enheten pasienten er hjemmehørende på – og som dermed har tjenstlig behov for opplysningene – får tilgang til denne pasientens journal. Når pasienten overflyttes til en annen enhet kan tilgangsrettighetene endres slik at det kun er den nye enhetens personell som får tilgang.

Ved å velge en slik løsning vil ansatte ved den enheten som pasienten er hjemmehørende på, få tilgang til all informasjon om pasienten som er registrert tidligere av andre enheter. Helsepersonell som arbeider ved helseinstitusjoner eller ved hjemmetjenestesoner i kommunen er å anse som "samarbeidende helsepersonell" iht. helsepersonelloven § 25 eller som "andre som yter helsehjelp" iht helsepersonelloven § 45. Lovens § 25 gir samarbeidende helsepersonell i samme virksomhet (her kommunen) adgang til å aksessere journalen på visse vilkår, mens helsepersonelloven § 45 sier at annet helsepersonell (dvs personell som behandler pasienten ved en senere anledning eller for et annet tilfelle/en annen episode) må be om å få tidligere opplysninger utlevert. I følge et høringsutkast fra SHdir sommeren 2006 til et rundskriv vedrørende utveksling av helseopplysninger internt i en virksomhet og mellom virksomheters elektroniske pasientjournalsystem, er det foreslått at utlevering av informasjon etter § 45 innenfor en virksomhet kan skje ved styring av tilgang. Det er dermed ikke krav om utlevering innenfor en virksomhet – dersom vilkårene for øvrig i § 45 er oppfylt.

Dersom det vurderes slik at de ansatte ved den nye enheten pasienten overføres til ikke skal ha tilgang til informasjon som tidligere enheter har lagt inn, må noen ved den enheten som har lagt inn informasjonen fortsatt ha tilgang til journalen etter at pasienten er flyttet til en annen avdeling. Dette vil muliggjøre framtidig utlevering. Det vil gjerne være mest naturlig at dette ivaretas av den som har rollen som journalansvarlig.

Se også henvendelse angående disse spørsmålene fra Stavanger kommune til Sosial- og helsedirektoratet av 27.06.2006, ref 7 i referanselista bak i dokumentet.

5.4.2 Urettmessig tilgang til (administrative) pasientopplysninger

Alt helsepersonell i kommunen som har tilgang til kommunikasjonsprogrammet som ble benyttet kan lese navn og personnummer på alle pasienter som det er sendt eller mottatt meldinger om, og kan redigere faste opplysninger på disse, selv om de ikke har et tjenestelig behov for dette. Hvis en bruker endrer opplysningene, vil det ikke logges hvem som har endret. Endringene blir alltid registrert på den første som har lagt inn en melding om pasienten i kommunikasjonsprogrammet. Både de gamle og de nye opplysningene blir liggende der.

Som minimum bør det logges hvem som gjør endringer. En integrasjon mellom kommunikasjonsprogrammet og fagsystemet vil også hjelpe på dette problemet. En mulighet vil være å fjerne visning av pasientoversikten i kommunikasjonsprogrammet, ev. fjerne den for vanlige brukere og kun gi slik tilgang til superbrukere.

Natttjenesten har fått mobil tilgang til all informasjon i fagsystemet for alle hjemmetjenestesoner. Personellet der kan derfor få tilgang til opplysninger om pasienter de ikke har behov for tilgang til. Natttjenesten er felles for alle soner, og har derfor potensielt behov for tilgang til informasjon om alle pasienter. Siden tilgangsstyringen er basert på personer og ikke på behov eller hendelser, har de ansatte tilgang til informasjon om alle selv om de ikke har tjenestelig behov for dette på det gitte tidspunkt. Et mulig tiltak for å endre dette vil være å knytte tilgangsrettighetene til vaktlistene, dvs at de som er på jobb kun får tilgang til de sonene de skal dekke den vakta. Det forutsetter at dette lar seg gjøre på en hensiktsmessig måte uten at det samtidig medfører hindringer for tilgang til opplysningene når det er behov for det.

Tilgang til "gamle" pasienter i kommunikasjonsprogrammet blir ikke fjernet. Informasjon blir liggende i arkivet på den enheten som brukeren tilhørte da meldingene ble sendt og mottatt. Dette medfører at brukerne etter hvert får tilgang til mye opplysninger de ikke har behov for tilgang til. Integrasjon av kommunikasjon i journalsystemet vil gjøre det mulig å regulere tilgangen til opplysninger bedre og på en mer enhetlig måte. Kommunikasjonsprogrammet vil da fungere som det det er tenkt til, nemlig et verktøy for sikker forsendelse av meldinger. Selve meldingene vil da bli liggende i fagsystemet, tilgjengelig for de som for øyeblikket deltar i omsorgen av pasienten. På den annen side vil slik integrasjon medføre at helsepersonell på nye enheter pasienten overføres til får tilgang til informasjon lagt inn av andre enheter, og som de ikke nødvendigvis trenger tilgang til. Ved bruk av kun ett journalsystem for hele kommunens pleie- og omsorgssektor, vil det muligens bli et større behov enn tidligere for å vurdere behovet for spering av journalnotat i den enkelte pasientjournal.

5.4.3 Manglende oppfølging fra fastleger

Av og til har pleiere opplevd at tilsynslegene og fastlegene ikke svarer på elektroniske henvendelser fra sykepleiere på sykehjem og i hjemmetjenesten. Enkelte leger følger ikke opp avtalte rutiner for gjennomgang av e-post fra sykehjem og hjemmetjenesten. Dette

medfører at systemet blir mindre brukt. Viktige ting tas per telefon og reseptbestillinger besvares stort sett i tide, men rutinesvikten medfører redusert tillit til løsningen.

For å sikre en mer stabil oppfølging fra legene, er det viktig å involvere hjelpepersonellet på legekantoret slik at de kan følge opp legene internt på legekantoret. Eventuelt kan man endre kravene for svarfrist slik at de er mer i tråd med legenes arbeidsrytme.

Noen legekantor vil ikke tilby elektronisk kommunikasjon med pleie- og omsorgssektoren fordi denne typen meldinger foreløpig ikke er integrert i journalsystemet. Legene må logge seg på kommunikasjonsprogrammet for å lese meldingene og eventuelt sende svar. Fast- og tilsynslegene i Tromsø kommune får epikriser, labsvar o.l. automatisk inn i innboksen i journalsystemet i dag (via kommunikasjonsprogrammet Well Communicator). De er ikke veldig motivert for å gå tilbake til en mer tungvint løsning med pålogging direkte på kommunikasjonsprogrammet for å få tilgang til meldinger fra hjemmetjenesten eller sykehjem. Denne type kommunikasjon bør integreres i legenes journalsystem for å gjøre det enklere for legene å ta i bruk tjenesten.

Kommunikasjonsprogrammet som ble benyttet har en funksjon for transportkvittering som gjør det mulig for den som sender en melding å se om kommunikasjonsprogrammet hos mottakeren har mottatt meldingen og klart å dekode den riktig. Meldinger som sendes fra kommunikasjonsprogrammet blir liggende i ut-mappa til de blir sendt ut. Etter at de er sendt ut fra kommunen blir de liggende i sendt-mappa inntil kommunikasjonsprogrammet mottar transportkvittering fra kommunikasjonsprogrammet hos mottaker om vellykket mottak og dekryptering av meldingen. Meldingen blir da flyttet fra sendt-mappa til akseptert-mappa. Systemet gir ikke noen feilmelding til brukerne dersom meldinger ikke kommer fram. Det er derfor viktig å sjekke sendt-mappa for å forsikre seg om at meldinger har blitt mottatt og akseptert av kommunikasjonsprogrammet hos mottaker.

5.4.4 Tap av kamera/kameraminnekort

Digitale kameraer er også attraktive tyveriobjekt. Det er derfor viktig med gode rutiner og regler for hvordan kamera og minnekort skal oppbevares og sikres. Rutiner for sletting av bilder på minnekort etter at bildene er lastet over i kommunikasjonsprogrammet er også viktig. Dette hindrer avsløring av pasientopplysninger hvis kamera med minnekort blir stjålet. For å øke sikkerheten ytterligere bør de ansatte som benytter digitalt kamera for å ta bilde av pasientenes sår instrueres til å ta bilder som så langt det er mulig ikke avslører identiteten til pasientene.

6. Forkortelser

EDGE	Står for Enhanced Data GSM Environment og er et mobilnett basert på en oppgradering av GSM-mobilnettet. Gjør at overføringshastigheten av data øker sammenlignet med det som oppnås på tradisjonell GSM. Har en maksimal teoretisk overføringshastighet på 200 Kbps
EDI-meldinger	Står for Electronic Data Interchange , eller på norsk Elektronisk Data Utveksling . Innebærer utveksling av informasjon mellom forskjellige programmer og systemer
GPRS	Står for General Packet Radio Service . Bruker mobilnettet og gir dataoverføring med maksimal teoretisk hastigheter på inntil 114 Kbps
HER-registeret	Helsetjeneste-Enhets-Registeret er en adressekatalog som viser adresser til de ulike enheter og personell innen helsevesenet som man kan kommunisere med
ICA	Står for Independent Computing Architecture og er en fjerntilgangsprotokoll brukt av Citrix Metaframe. Citrix ICA benytter TCP-port 1494.
LAN	Står for Local Area Network . Med LAN menes firmaets eller organisasjonens private kablede datanettverk.
PCMCIA	Står for Personal Computer Memory Card International Association . Dette er en organisasjon som lager standarder for ekstrastyr til bærbare datamaskiner. PCMCIA-ekstrastyr er en type maskinvare som kan kobles til en bærbar datamaskin hvis den har en PCMCIA-port.
SSL	Står for Secure Sockets Layer . Dette er en protokoll for å overføre sensitiv informasjon over Internett. SSL bruker en krypteringssystem som bruker en privat nøkkel og en offentlig nøkkel.
UMTS	Står for Universal Mobile Telecommunications System . Mobilnett som gjør at data kan overføres 8-10 ganger raskere enn i GSM-nettet, maksimal teoretisk overføringshastighet på 384 Kbps.

7. Referanser

1. Daniel Nygård og Harald Øverli Eriksen, NST m. fl.: *"Teknisk beskrivelse – SES@m Tromsø-prosjektet"*
2. Harald Øverli Eriksen, NST m.fl.: *"Tekniske erfaringer – SES@m Tromsø-prosjektet"*
3. Line Nordgård, NST: *"Opplæring Oppfølging – Erfaringer fra opplærings- og oppfølgingsarbeidet ved implementeringen av de telemedisinske samhandlings-tjenestene i SES@m Tromsø."*
4. Leif E. Nohr, NST: *"Juridiske problemstillinger i elektronisk samhandlingsprosjektet - SES@m Tromsø"*
5. Jussrapport – Stavanger – Kommunalt fyrtårn for elektronisk samarbeid på helse- og sosialtjenesteområdet, 27-06-2006. http://www.shdir.no/samspill/kommuneprogram/fyrt_rnsjuss__51769

De fire første dokumentene i lista over er publisert på SES@m Tromsø-prosjektets web-side: <http://www.telemed.no/cparticle195396-30410.html>