Nasjonalt senter for telemedisin
Regionsykehuset i Tromsø

Nasjonalt senter for telemedisin
Regionsykehuset i Tromsø

Tittel Nordmail. Oppnås en bedre koordinasjon og kommunikasjon mellom hjemmetjeneste og fastlege ved bruk av PKI-sikret e-mail?	**NST – rapport** 04-2002 **ISBN** 82-92092-05-6 **Antall sider** 72 **Dato 11/2-02** 27.05.2002
Forfattere Siri Birgitte Uldal	
Emneord E-post, hjemmetjenesten, primærlege, pasientkommunikasjon	
Sammendrag Se s. 4	
Title Nordmail: Will PKI-based e-mail improve communication between home care institutions and general practitioners?	
Abstract	

Nasjonalt senter for telemedisin, 2002

ISBN 82-92092-05-6

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

Universitetssykehuset Nord-Norge HF
Nasjonalt senter for telemedisin
Postboks 35
9038 Tromsø
http://www.telemed.no

Forord

Tanken bak denne prosjektrapporten er å samle opp erfaringene fra Nordmail prosjeket slik at disse kan utnyttes og videreforedles i andre prosjekter. Rapporten sammenfatter derfor både utførelse, metode og en vurdering av prosjektet i ettertid sammen med rene tekniske beskrivelser. De tekniske beskrivelsene er først og fremst rettet mot personell med teknisk bakgrunn/erfaring og helsepersonell vil derfor kanskje velge å hoppe over disse.

Prosjektet var internfinansiert av NST og var koordinert med parallelle aktiviter.

Takk til prosjektdeltagere i Tromsø kommune og ansatte ved Stakkevollan og Nordbyen legesenter for deltagelse, postiv innstilling og vilje til å arbeide fram Nordmail.

INNHOLD

Sammendrag

Kan kommunikasjon og koordinasjon mellom hjemmetjeneste og fastlege bedres ved bruk av elektronisk post? Spørsmålet skulle vært undersøkt i Nordmail prosjektet. Prosjektet skulle testet ut bruk av sikret e-post kommunikasjon mellom personell ved Nordbyen og Stakkevollan legesentre og Guleng og Stakkevollan hjemmetjeneste.

Krav i prosjektet var at nettverket skulle tilknyttes Nordnorsk Helsenett (NH) og tilfredsstille lovverkets krav til sikkerhet (håndhevet av Datatilsynet) for overføring av sensitive opplysninger. Det siste kravet viste seg imidlertid å være vanskeligere enn vi hadde trodd uten å ta i bruk terminalservere og tynne klienter. Prosjektet ble forvansket ved at mange strukturer var i forandring samtidig som prosjektet dro ut i langdrag. Til tross for en svært positiv innstilling hos alle involverte, tok det tid å oppdatere involverte prosjektdeltagere samtidig som arbeidet med å finne en akseptabel teknisk løsning pågikk "på overtid". Dette var hovedårsak til prosjektnedleggelse.

Erfaringene fra prosjektet har imdlertid vært nyttige. NST fikk kjennskap til hvordan hjemmetjenesten og allmenpraktikerne arbeider. Resultatene fra denne prosessen er blant annet en nesten ferdig mal for sikkerhetshåndbok for små helseinstitusjoner tilknyttet NH.

Rapporten sammenfatter bakgrunn og metoder brukt i prosjektet, tenkt analysering/evaluering, tekniske problemstillinger og resultat.

Kommentar

1.1.2001 skiftet Regionsykehuset i Tromsø eier og navn til Universitetssykehuset Nord-Norge Helseforetak. For å unngå forvirring brukes sistnevnte betegnelse konsekvent.

Ordliste

Asymmetrisk kryptografi	Asymmetriske nøkler er basert på strukturer av offentlige og private nøkkelsystem. Nøklene er elektroniske og opptrer i par, hvorav den ene er offentlig kjent, mens den andre er privat og hemmelig. Den hemmelige nøkkelen gis aldri ut; mottaker bruker offentlig nøkkel til dekryptering.
Autentisering	Bekreftelse av en oppgitt identitet. Her: å identifisere seg selv mot datanettverket.
Blowfish	Blokkalgoritme for kryptering laget av Bruce Schneider. Algoritmen tillater variable nøkler opp til 448 bits og er upatentert.
CA	Certification Authority. En CA utsteder et digitalt sertifikat ved å knytte nøkler til en person/identitet og bekrefter at innholdet i sertifikatet er riktig.
DES /DES128	Data Encryption Standard er en blokkalgoritme som bruker 56-bits nøkkel og har flere operasjonsmodi avhengig av bruksområde. DES128 har som navnet sier 128-bits nøkler.
Diffie-Hellman	En metode for sikret utveksling av delte private nøkler.
Digital signatur	Attestering av elektronisk dokument.
DORIS	Multimediasystem for bruk i telemedisinske tjenester, utviklet for helsevesenet av NST og Well Diagnostics.
GSM	Global System for Mobile Communications, en av verdens mest utbredte kommunikasjonssystemer for mobil telefoni. GSM ble introdusert i 1991.
Helseradio	Eldre kommunikasjonssystem til bruk innen norsk helsevesen.
HTTP/HTTPS	Hyper Text Transfer Protocol brukes for å overføre dokumenter lagret på andre datamaskiner (web-servere). HTTPS er en (SSL) sikret utgave av HTTP.
IETF	Internet Engineering Task Force.
IPsec	Internet Engineering Task Force (IETF)'s IP sikkerhetsprotokoll. IPsec definerer et sett av spesifikasjoner for kryptografi-basert autentisering, integritet og konfidensialitet på IP laget.
IP	Internet Protocol. Del av firelags-modell som beskriver kommunikasjon med internett teknologi.
ITU	International Telecommunication Union.
KITH	Kompetansesenter for IT i helsevesenet.

Kryptering	Koding av meldinger slik at de blir uleselige for uvedkommende.
NH	Nordnorsk Helsenett, brukt både om det fylkeskommunale selskapet og om datanettverket mellom helseinstitusjoner.
NSD	Norsk Samfunnsvitenskapelig Datatjenste.
NST	Nasjonalt senter for telemedisin.
PGP	Pretty Good Privacy er et offentlig nøkkel krypteringsprogram, skrevet av Phil Zimmermann i 1991. Programmet er fritt tilgjengelig på Internett og har blitt en uoffisiell standard for kryptering av privatpersoners e-post.
PKCS	Public-Key Cryptography Standards spesifisert av RSA Laboratories sammen med partnere. Publisert første gang i 1991. PKCS har ført til mange formelle og de facto standarder innen sikkerhet inkludert SET og SSL.
PKCS#11	PKCS #11 er standard for tilkopling av identifikasjon (token) som for eksempel smartkort. Standarden definerer et programmeringsgrensesnitt (API) kalt Cryptoki som inneholder kryptografisk informasjon og utfører kryptografiske funksjoner.
PKI	Public Key Infrastructure er basert på asymmetriske nøkkelstrukturer. Strukturens hensikt er å håndtere nøkler og sertifikater slik at elektroniske transaksjoner kan utføres med tillit mellom aktørene.
PRO	Pleie, rehabilitering og omsorg.
RA	Registration Authority. En RA registrerer brukere og bekrefter (fysisk deres) identitet ved forespørsel om sertifikat, men vil aldri selv utstede og signere sertifikater.
RC4	Algoritme basert på streams heller enn blokker. Algoritmen er utviklet av Ronald Rivest og holdt hemmelig av RSA Data Security, men ble kompromittert i 1994. RC4 tillater fra 1 til 2048 bits på nøkler.
RC5	Blokk algoritme utviklet av Ronald Rivest, publiert i 1994. RC5 tillater variabel nøkkellengde, data blokk størrelse og data krypteringsrunder.
Rejndael	Rijndael er en blokk kryptering laget av Joan Daemen og Vincent Rijmen. Krypteringen kan ha variable blokk og nøkkellengde. Hittil er nøkkel- og blokklengder implementert i 128, 192, or 256 bits
RDP	Remote Desktop Protocol er en protokoll for terminalserving. Det er RDP som gir mulighet for scrolling av et dokument på server

	etter som server sender skjermoppdateringer til klient. Tastatur og musbevegelser overføres også via RDP protokollen.
RSA	RSA er en asymmetrisk krypteringsalgoritme utviklet i 1997 av Ronald Rivest, Adi Shamir og Leonard Adleman. Algoritmen kan brukes både for informasjonskryptering og som basis for digiale signaturer/autentisering. Nøkkellengden til algoritmen kan variere.
Secure ICA	Secure Independent Computing Architecture er en terminalserver/tynn klient løsning med støtte for RC5. Ved siden av sikkerhet, gir protokollen mulighet for scrolling av et dokument på server etter som server sender skjermoppdateringer til klient ved siden av bl.a. tastatur- og musbevegelser.
SEIS	Secured Electronic Information in Society. Svensk forening som bl.a. har utarbeidet en standard serifikatprofil.
SET	Secure Electronic Transaction er en kryptografisk protokoll for overføring av krypterte kredittkortnummer over Internett.
SHD	Sosial- og helsedepartementet
SPKI	Simple Public Mail Infrastructure. Et sertifikat format laget av SPKI arbeidsgruppen i IETF.
SSL	Secure Socket Layer er en portokoll laget av Netscape Communication Corporation for å sikre toveis kommunikasjon av en forbindelse gjennom kryptering, autentisering og integritet.
Symmetrisk kryptografi	Krypteringsmetode hvor samme nøkkel brukes ved både kryptering og dekryptering.
T.120	T.120 er en protokoll for overføring av multimedia data.
TCP	Transmission Control Protocol er en overføringsprotokoll som også sjekker at informasjon er overført og sørger for retransmisjon om nødvendig. TCP bruker IP til å flytte pakker rundt i nettverket.
Terminal server	En terminalserver er karakterisert ved at ingen programmer eller data overføres til klienten annet enn skjermoppdatering og utskriftsdata. Terminalserveren utfører alle programmer og behandler data på vegne av klienten.
TTP	En tiltrodd tredjepart. Inkluderer bl.a. CA og eventuelt RA.
Tynn klient	Tynn klient kalles en applikasjon som utfører kommunikasjon mot en terminalserver.
UNN	Universitetssykehuset i Nord-Norge HF
URL	Uniform Resource Locator er en unik karakterstreng som peker til et unikt sted på Internett (dvs. en Internett adresse).
X.509	En sertifikatstandard som kan brukes både ved autentisering, kryptering og signering i en PKI løsning.

Kort prosjektbeskrivelse

En uformell forundersøkelse viste at personell ved Stakkevollan og Guleng hjemmetjenester i Tromsø har en travel hverdag. Det samme gjelder personell ved Nordbyen og Stakkevollan legesentre, som til enhver tid har ca 20-40 felles pasienter med hjemmetjenestene. God samhandling er viktig for pasientene. I dag er dette vanskeliggjort blant annet fordi fastlege og hjemmetjeneste ikke har noen felles møteplasser. Hjemmetjenestens folk ringer av og til når det er pasienter inne hos legen. Da har legen dårlig tid og må gi raske svar som sjelden kvalitetssikres ved oppslag i journal. Hjemmesykepleierne opplever usikkerhet omkring medisindosene når denne kun er angis muntlig over telefon. Den skriftlige kommunikasjon kommer ofte sent fram. Mangel på kontakt mellom helsearbeidere øker faren for at pasientene kan forverre sin sykdomstilstand på grunn av feilbehandling.

Prosjektets mål var å undersøke om kommunikasjon og koordinasjon mellom hjemmetjeneste og fastlege kunne bedres ved bruk av elektronisk post. Posten skulle være sikret mot innsyn fra uvedkommende (kryptering), beskyttet mot endring underveis (kontrollmelding) og attestert av rette vedkommende (digital signatur). Deltakerinstitusjonene skulle koples til Nordnorsk Helsenett (NH), internettverket for helsearbeidere i Nordland, Troms og Finnmark. Det var planlagt at både allmenpraktikerne og hjemmetjenesten skulle få tilgang til fagnettverk via Internett. Vedlegg 1 inneholder protokoll.

Krav til prosjektet

-Fastlegene ønsket tilknytning til NH. Gjennom tilknytning til NH fås også tilgang til Internett.

-Innhente samtykke fra Datatilsynet. For å få akseptanse som forskning, skulle det innhentes samtykke fra Statens Helsetilsyn og Norsk Samfunnsvitenskapelig Datatjeneste. Regional komite for medisinsk forskingsetikk skulle forespørres.

- ”Felles postkasse” for e-post mottak til hver institusjon.

-Om nødvendig innføre restriksjoner på bruk av e-post. Eventuelle restriksjoner kunne omhandle frekvens, organisering rundt bruk og innhold. Restriksjonene skulle vurderes etter et par ukers utprøvning.

-Utstyr bekostes av NST og beholdes av brukerne etter ferdig undersøkelse. Til gjengjeld stiller brukerne opp på analyse/evaluering i forbindelse med prøveprosjektet.

Prosjektets historie

1999: NST fikk i 1999 tilført økte bevilgninger over statsbudsjettet. Det ble opprettet en eget område for pasientnære tjenester.

Nov 1999: Forfatteren av dette dokumentet hospiterte en dag ved Guleng og Stakkevollan hjemmetjeneste. Samtidig diskuterte vi muligheter og behov for

telemedisin i hjemmetjenesten. Hjemmetjenestens personell ønsket seg bedre kontakt med fastlege. Sikker e-post mellom de to kunne være en løsning på problemet. Stakkevollan og Nordbyen legesentre var de fastlegene Guleng og Stakkevollan hjemmetjeneste hadde flest pasienter felles med.

Etter hospiteringen ønsket NST å starte opp e-post kommunikasjon mellom hjemmetjeneste og fastlege forutsatt at vi fikk brukere med oss. I kommunen var det mange som måtte involveres: Foruten soneleder for Stakkevollan og Guleng hjemmetjeneste skulle områdeleder, PRO sjef og helsesjef informeres. I tillegg skulle kommunens IT avdeling involveres. Hjemmetjenestene på Tromsøya hadde innføring av journalen Profil nær forestående, slik at NST måtte koordinere seg med prosjektleder.

Færre personer var involvert på fastlegesiden. Hvert legesenter hadde sin representant som både var en del av ledelsen og var dataansvarlig.

Jan 1999: Litteraturstudie og første utkast til protokoll.

Oppstartsmøte i Nordmail prosjektet der endel innledende opplysninger, ønsker og avklaringer ble gjort. Ansatte på legesenterene ønsket seg en kvalitativ evaluering, mens hjemmetjenestens personale ønsket intervju. Oppstart for oppkopling i prosjektet ble satt til februar 2000. Felles prosjektmøter ville bli vanskelig å få gjennomført fordi møtene da måtte legges på overtid. Det var enklere for brukerne at NST oppdaterte og informerte gjennom besøk/telefon hos hver av institusjonene.

Feb 2000: Datatilsynet kom ut med første veiledning for små helseinstitusjoner. Alle mindre helseinstitusjoner må søke Datatilsynet om godkjenning for tilknytning til eksterne nett. Samtale med Datatilsynet avklarte at e-post adresser tilknyttet funksjonalitet var akseptabelt.

2. versjon av protokoll klar med forskjøvede tidsfrister (oppkopling sept 2000). Kvalitative evalueringsmetoder ble valgt (se eget avsnitt).

Aug 2000: NST har ansatt sikkerhetsrådgiver.

Sept. 2000: Kommunens IT avdeling tar i bruk terminalservere ved innføring av brukerjournalen Profil og sikret tilgang til Internett på Guleng og Stakkevollan hjemmetjenester.

Siri Andersen er kommet tilbake som soneleder på Guleng etter Camilla Børresen. To av legene ved Stakkevollan legesenter avtrer sine stillinger, Trond Brattland overtar som dataansvarlig etter Charlotte Goll. På Stakkevollan hjemmetjeneste er Else Thoril Nielsen og Anne Katrine Johansen utpekt som dataansvarlige. Siri Andersen og Elisabeth Sausjord er dataansvarlige for Guleng. I forbindelse med nyansettelser oppdateres hjemmetjenesten og Stakkevollan legesenter.

Okt 2000: Datatilsynet kommer ut med veiledning om bruk av tynne klienter for å skille eksterne, interne og sikre soner.

Profil innføres på Tromsøya og taes i bruk på Stakkevollan og Guleng hjemmetjeneste.

Statens Helsetilsyn søkes for oppstart i prosjektet. Det er på forhånd avklart med Regional komite for medisinsk forskningsetikk at søknaden faller utenfor deres virkefelt.

Nov 2000: Søknad sendes Datatilsynet. I forbindelse med søknaden intervjuer prosjektleder flere avdelinger innen kommunen, hjemmetjenesten og dataansvarlig på Stakkevollan og Nordbyen legesentre mm. Det arbeides med å komme fram til en teknisk løsning.

Des 2000: NH skilles ut fra NST som et eget fylkeskommunalt selskap. Stilling som daglig leder utlyses.

Jan 2001: Tilbakemelding fra Datatilsynet om at søknadsrapport er grundig, men for lang. Ny søknadsrunde startes.

Konsulenter fra KPMG innleies til å få satt opp drifts- og sikkerhetsrutiner for NH. Som fylkeskommunalt selskap løsrevet fra Universitetssykehuset Nord-Norge ønsker Datatilsynet i utgangspunktet ikke å vurdere NHs sikkerhetsløsninger.

Nye forskrifter fra Datatilsynet som følge av nytt lovverk [1]. Meldeplikt innføres istedet for søknad om godkjenning. Fram til 2002 kan fortsatt søknader om godkjenning sendes inn.

*Feb 2001: "*Administrativ veiledning for mindre virksomheter" utarbeidet av Ecsoft Norge AS og System Sikkerhet AS på oppdrag av SHD utgis.

KITHs rapport om SESAM (Sikker elektronisk samhanding på Aker sykehus) utgis [2]. Her er PKI-løsning utprøvd i mellom Bjerke hjemmetjeneste og Aker sykehus, men institusjonene har ikke samtidig tilgang til Internett.

Norsk Samfunnsvitenskaplig Datatjeneste (NSD) ønsker likevel en søknad fra prosjektet. Søknad sendes.

Mars 2001: Svar fra NSD med anbefaling om at prosjektet gis konsesjon, men avventer respons fra Datatilsynet.

April 2001: Henvendelse fra Berit Rosenvinge, overlege alderspsykiatrisk post/sektoroverlege supraregional sektor. Hun ønsker bedre kontakt med hjemmetjenesten og allmenpraktiker ved oppfølging av psykiatriske pasienter for å hindre unødvendig innleggelser på Åsgård psykiatriske sykehus. Dette kan kanskje løses gjennom bruk av sikret e-post.

Statens Helsetilsyn avslår søknad om evaluators innsyn i e-post generert i prosjektet til bruk ved analyse/evaluering.

Mai 2001: Datatilsynet avslår søknad om evaluators innsyn i e-post generert i prosjektet til bruk ved analyse/evaluering. Prosjektet kan likevel videreføres ved at hjemmetjenesten og fastlege anonymiserer data før innsyn.

NH og NST får Zebsigns PKI-løsning for utprøving. Disse vil kunne brukes sammen med terminalserverløsningen for overføring av sikker e-post.

Juni 2001: Datatilsynet aksepterer å vurdere NHs sikkerhetsløsninger sett fra en mindre helseinstitusjons ståsted. Nordbyen legesenter velges som eksempel. Sikkerhetshåndbok ferdigstilles med unntak av aksepterte tekniske løsninger for sikker e-post kommunikasjon.

I et møte fronter Datatilsynet terminalservere som en løsning på teknisk oppsett.

Sept 2001: Guleng og Stakkevollan hjemmetjenester flytter ned til nye lokaler på Seminartomta.

NH ønsker ikke å benytte terminalservere for teknisk infrastruktur, og vil se på andre løsninger. Datatilsynet er åpen for forslag, men disse må gjennomgåes grundig. Samtidig har kommunens IT avdeling valgt å basere sin nettsikkerhet på terminalservere, noe som forvansker sammenkopling mellom NH og kommunens datanett. For å få Nordmail prosjektet igangsatt kreves nå en lengre prosess mot Datatilsynet sammen med kommunens IT avdeling for å finne alternative sikkerhetsløsninger. Nordmail prosjektet er allerede mer enn ett år forsinket. Prosjektleder søker NSTs lederteam om nedleggelse for å slippe å holde på brukerne i et prosjekt det er uvisst når kan realiseres.

Okt/nov 2001: Lederteamet ved NST vedtar å nedlegge Nordmail prosjektet.

Styringsverktøy og prosjektmetoder

Prosjektet ble innledet med hospitering både i hjemmetjenesten og hos allmenpraktiker. Hospiteringen fungerte som et middel til å forstå hverdagen for hjemmetjenestens folk og for allmenpraktikere, samtidig som det gav mulighet for diskusjoner omkring nytteverdi og valg av mulige telemedisinprosjekt.

Protokoll med tids- og kostnadsplan samt beskrivelse ble laget. Ettersom prosjektet involverte mange partnere, ble det ført dagbok over framdrift, innspill og hvem som skal kontaktes når. Det ble også ført teknisk dagbok over teknologier som er blitt vurdert og som enten skal forkastes eller arbeides videre med.

I tillegg til protokoll ble Nordmail prosjektet brukt som eksempel i forbindelse med BI kurs om prosjektledelse våren 2001. Det ble utarbeidet aktivitetsliste, nettverksdiagram, ressursdiagram, tids- og ansvarskart og GANT-diagram.

Nøkkelpersoner/institusjoner

- Helsesjef
  - PROsjef
- Områdeleder
- Soneledere, sikkerhetsansvarlige og nestansvarlige på Stakkevollan og Guleng hjemmetjenester.
- Kommunens IT avdeling
- Berit Rosenvinge/ overlege alderspsykiatrisk post / sektoroverlege supraregional sektor
- Leger og helsesekretærer på Stakkevollan og Nordbyen legesenter.
- Prosjektleder for innføring av Profil på Tromsøya.
- Norsk samfunnsvitenskapelig datatjeneste, Datatilsynet og Statens helsetilsyn.

-Overordnede og personer som arbeider med relaterte prosjekter på NST.
-Sjef og teknisk ansvarlige på NH.
-IT avdeling Alta kommune (for ønske om parallelt prosjekt i Alta.)

Erfaringer fra prosjektet gjennom hospitering og samtaler med helsepersonell

Okt 1999: Hospitering på Guleng og Stakkevollan hjemmetjeneste

Gjøremål /daglige rutiner
Hjemmetjenestens sykepleiere, hjelpepleiere, omsorgsarbeidere og ufaglærte går visitter, avhengig av brukers behov. Det er hjemmetjenestens erfarne folk som skriver førstegangsrapport, som skal være mer grundig enn de etterfølgende rapportene. Soneleder er som regel på hjemmetjenestens lokaler og tar imot forspørsler og arbeider med administrasjon. Det er sjelden soneleder skriver førstegangsrapport, eller selv får tid til å gå visitter (gjøres av og til hvis sonen er liten).

Hjemmesykepleierne er ansvarlig for medikamentering overfor syke pasienter.
Både sykepleiere, hjelpepleiere, omsorgsarbeidere og ufaglærte har adgang til og bruker journalen Profil aktivt. Soneleder er sannsynligvis den som benytter Profil mest. Personell som er mye ute hos brukere, er ofte de første til å merke forandring i sykdomsbilde hos pasient, samtidig som overlevering gjerne skjer muntlig til soneleder eller i rapporteringsmøter.

Lagrede sensitive opplysninger
Da prosjektet startet, brukte hjemmetjenesten fire skjema for brukere. Det ene skjemaet omhandlet medisinering. Alle disse skjemaene finnes nå i Profil.

Rapport om fysiske, psykiske og sosiale forhold. Her inngår en beskrivelse av førsteinntrykket av pasientens tilstand; fysisk, psykisk, sosialt kontaktnettverk, utgangspunkt for behandling osv. Rapport utfylles første gang av fagutviklingssykepleier eller soneleder og oppfølges siden av primærkontakten (hjemmetjenesten har en sykepleier eller hjelpepleier som er ansvarlig for hver pasient, selv om ikke pasienten alltid besøkes av primærkontakten). Av og til er ikke disse rapportene helt oppdaterte. Det kan være vanskelig for hjemmetjenestens arbeidere, som ofte følger brukeren tett å legge merke til forandringer som skjer gradvis. Det finnes ikke i dag noe formelt krav om hvor ofte rapport skal oppdateres. Men det skal skje når sykepleier eller hjelpepleier merker forandringer. For eksempel er det ikke nødvendig å skrive ned dagligdagse ting som ”spist godt” dersom matlyst ikke er noe problem for bruker.

Hjemmesykepleiens hovedkort. Kontaktopplysninger, opplysninger om hjelpemidler, institusjonsopphold, diett, cave mm. En rubrikk er merket ”oppdragets art” utfylles med hva hjemmetjenesten skal gjøre for bruker. Behov varierer fra kun å gi ut doseringseske med medisiner en gang i uka til besøk opptil 7 ganger i døgnet.

Daglig rapport. Den som har besøkt bruker (sykepleier, hjelpepleier, ufaglært) fører sykepleierdokumentasjon over pasientens tilstand. Daglig rapport er et eksempel på dokumentasjon som skrives på en annen måte enn hva legen etterspør. Legen vil gjerne ha en kort ”tilstandsrapport” på 1-2 linjer; men fordi hjemmetjenestens folk følger pasient nært over tid, vil beskrivelsene hos hjemmetjenesten ofte bli omfattende.

Medisinering. Dette skjemaet inneholder informasjon om medisinering og seponering og hvilken lege som har ordinert medisinene.

I tillegg finnes det endel andre viktige dokumenter for hjemmetjenesten på data:
-Wordmaler omkring vakt/turuslister. Her inngår ingen pasientopplysninger.
-Stelleplan for den enkelte pasient. Det er også en mengde brev, hvorav endel inneholder sensitive opplysninger.
- Hjemmetjenestens folk må ha med seg papirer med sensitiv informasjon når de er på visitter. F.eks. må ansatte ha tilgang til telefonliste for alle brukerne; på denne lista står også en kort beskrivelse av pleieplan. Lista taes med på kvelds- og nattevakter, og det er selvsagt en viss fare for at den kan bli gjenglemt. Listene samles imidlertid inn igjen etterpå, slik at tap vil oppdages. På dagtid kan opplysningene skaffes ved å ringe sekretær på hjemmetjenesten.
-På kvelds- og nattevakter skal en ansatt ha med seg en vakttelefon (GSM mobiltelefon) som legevakta benytter seg av ved kontakt med hjemmetjenesten for eksempel når en trygghetsalarm blir utløst. Hjemmetjenesten har med seg et papir der hver bruker er tildelt en kode. Før brukte hjemmetjenesten helseradio.

Behov sett fra ansatte ved Stakkevollan og Guleng hjemmetjeneste (mulige nye telemedisin prosjekter)
Basisopplysninger som primærlege ev. legevakt vil kunne ha hvis pasient er henvist:
-Navn, adresse, tlf, fødselsdato, pårørendeopplysninger, nabokontakt.
-Diagnose, diett, cave.
-Hvem pasienten er henvist fra (lege, legesenter).
-Behandlende lege hvis ikke dette er den samme som henviser.
I dag må hjemmetjenesten enten få disse opplysningene av pasient eller pårørende hvis det ikke er legen som henviser. Hvis lege henviser, kommer opplysningene med vanlig posttjeneste. Hvis pårørende eller pasient selv tar kontakt, vil hjemmetjenesten dra til bruker for vurderingsbesøk. Dersom det er viktig å innhente opplysninger fra primærlegen, spørres pasient om lov til å kontakte lege via telefon eller brev.

- Hjemmetjenesten må få beskjed av lege om medisinering hvis hjemmetjenestens folk skal være ansvarlig for medisinutdeling og administrering. I dag gis dette i nødsfall muntlig over telefon selv om dette ikke er ønskelig (pga feilskrivinger/oppfattelser samt større mulighet for ansvarsfraskrivelse ved feilmedisinering). Hvis det er pårørende som kontakter hjemmetjenesten, tar hjemmetjenesten kontakt med legen hvis pasient aksepterer dette. Hjemmetjenesten må ha ordinering fra lege før de kan dosere. Er det pårørende som tar seg av medisinering, har hjemmetjenesten intet ansvar. Hjemmetjenesten avtaler skriftlig med pasient hvem som skal være ansvarlige for å dosere og hente medisiner (her har hjemmetjenesten et eget skjema).

-Labresultater: både fra primærlege og sykehus: blodprøver og urinprøver, men overføring kan ikke skje automatisk. I dag ringer hjemmetjenesten primærlege hvis pasient aksepterer det.

-Ved reseptoverføringer ser det ut til å være lite å hente for hjemmetjenesten ved digitalisering. Hjemmetjenestene har kontrakt med Svaneapoteket som både henter resepter og bringer ut medisiner en gang i uka. Hvis en pasient kommer med resept til hjemmetjenesten og ber hjemmetjenesten ta hånd om medisineringen, kan denne resepten sendes med apotekets bud. Av og til gir hjemmetjenesten allmenpraktiker beskjed om å sende resept direkte til apotek, hvor hjemmetjenesten får medisinene tilbake etterpå ved levering. Da fakses resepten fra fastlegen, men med faks får man kun

en forpakning. Hvis PKI løsninger åpner for digital overføring der reiterasjon (mulighet for å bruke samme resept ved flere medisinuttak) er tillatt, vil dette kunne forenkle hverdagen til hjemmetjenesten. Det er Statens helsetilsyn som i dag vurderer når reiterasjon er tillatt.

-Hjemmetjenestens folk kunne også ønske et system for påminning om henting av nye medisiner/når lege skal kontaktes for nye resepter. Det samme kunne de ønske for legesenterene, slik at hjemmetjenestens folk var sikker på at resept lå klar ved henting.

Opplysninger fra hjelpemiddelsentralen til hjemmetjenesten:
-Hvilke hjelpemidler pasienten har fått utdelt. Det kan også hende at hjelpemiddelsentralen ikke har korrekte opplysninger om hjelpemidler. F.eks. er det endel pasienter som ikke bruker hjelpemidlene de har fått utlevert. Da vil hjemmetjenesten sitte med opplysninger potensielt av interesse for hjelpemiddelsentralen.

Des 1999: Hospitering på Nordbyen legesenter

Gjøremål /daglige rutiner
Nordbyen legesenter starter dagen med morgenmøter fra kl. 8.00 til 8.30 der dagsaktuelle saker taes opp. Legene starter med pasientene kl 8.30. Endel av pasientene kommer med psykiske lidelser, rusproblemer eller underlivssykdommer; noe som gjør det ekstra vanskelig for lege og ubehagelig for pasient å bli avbrutt.

Legene har telefontid for pasientene en halv time hver, stort sett daglig. Da prosjektleder hospiterte, stod ikke telefonen stille mer enn i noen få sekunder. Ingen leger har telefontreffetid i samme tidsrom.

Matpausene skal være på 30 min, men blir ofte kortere. Lunsjen brukes gjerne til å oppdatere seg på kollegers arbeide. Etter lunsj fortsetter legene med pasientkonsultasjoner fram til ca. kl. 15.00, noen ganger til kl. 16.00. Etter siste pasient har legene en del oppfølgende arbeid å gjøre, som å skrive ferdig journalnotater, skrive erklæringer, sykemeldinger, ringe pasienter mm. Det er på denne tiden det passer legene best at hjemmetjenestens folk ringer.

Alle henvendelser fra samarbeidspartnere (fysioterapeut, hjemmetjeneste, sosialkontor, helsestasjon, sykehus osv) går direkte inn til lege.Typiske henvendelser fra hjemmetjenesten er forespørsel om endret medisinering.

Antallet pasienter for hver fastlege er bl.a. avhengig av aldersfordeling. Unni Ringberg, Terese Fors og Trygve Deraas har mest eldre pasienter med tilknytning til hjemmetjenesten. De har også mange med psykiske lidelser og rusmisbrukere, pasientkategorier som må regnes som ”tunge”.

AMK og legevakt ringer ofte til legesenteret for akutthenvisninger for eksempel med båtfolk, turister og andre uten fastlege i Tromsø. (Det finnes ingen retningslinjer for hvilke legesentre som kan bli oppringt). Disse øyeblikkelig hjelp-pasientene utgjør en viss andel av kvoten på 18-22 timer pr. uke som Nordbyen legesenter har avsatt. Utover øyeblikkelig hjelp kvoten tar det ca 2-5 uker å komme til lege.

Kommunikasjon med Universitetssykehuset i Nord-Norge HF (UNN): Rekvisisjon på f.eks. en røntgen undersøkelse hentes daglig av bud fra UNN. Røntgenavdelingen bestemmer time, og gir beskjed til pasient. Etter timen sendes røntgensvar tilbake til

primærlege på papir. Epikrisepapiret kastes etter at helsesekretærene har scannet inn epikrisen i den elektroniske journalen.

Legesekretærene tar alt av blodprøver, urinprøver, EKG, sårskift mm. etter delegering. De gjør booking og skriver ut resepter på faste medisiner som legen må signere. Dessuten er de ansvarlige for mottak av labsvarprøver fra UNN elektronisk, og forsendelser av labprøver til UNN (som går med bud). I tillegg kommer dokumentasjons- og papirarbeide.

Hvis resept er dosert for flere enn en gang, må hjemmetjenesten selv hente resepten, i motsatt tilfelle fakses denne til apotek direkte. Hjemmetjenesten betaler ikke for resept når de henter resepten. (Legesentrene sender ut regning direkte til bruker, en tjeneste som er relativt kostbar.) For helsesekretærene fungerer ikke alltid kontakten med hjemmetjenesten: Samme resept kan bli ringt inn flere ganger fra hjemmetjenesten, eller hjemmetjenesten kommer ikke for å hente en resept.

Lagrede sensitive opplysninger
Først og fremst pasientjournal. Men legesenteret oppbevarer også lange epikriser på papir og skriver kun et kort sammendrag inn i ProfDoc. Dette kan være både laboratoriesvar og svar fra andre kontor.

Brev og rapporter som skrives med sensitivt innhold lagres alltid på server.

Behov sett fra ansatte på Nordbyen legesenter (mulige nye telemedisin prosjekter)
-Først og fremst er det et behov for oppdatert liste om medisinering i fall en annen lege har forskrevet ny medisinering. Denne bør komme elektronisk direkte fra legen, men hvis hjemmetjenesten har utløst forespørselen (f.eks. i løpet av nattevakten), kan eventuelt hjemmetjenesten gi midlertidig beskjed.

- Personell på Nordbyen legesenter ønsket at pasienter selv kan gjøre timebestillinger (bortsett fra øyeblikkelig hjelp-timene).

-Primærlegene ønsket sikker elektronisk kommunikasjon til spesialistene på UNN. Dette gjelder mot nesten alle sykehusavdelingene.

Opplysninger fra hjemmetjenesten som primærlege/sykehus kunne ha behov for:
-Fastlegen ønsker beskjed hvis en pasient er blitt bruker av hjemmetjenesten (hvis henvisning kommer fra andre).
-Hvem som henviste pasient til hjemmetjenesten (hvis dette ikke var fastlegen).
-Den/de spesialistene som har behandlet pasient på sykehus, eventuelt hvilken legevaktslege det var.

-Sykepleier fører dagbok over pasientens tilstand. Denne kan være interessant for lege, samtidig som leger etterspør et kort ekstrakt. Fordi sykepleierne følger pasienten nøye over tid, vil informasjonen bli anderledes enn det legen etterspør. Skjema-standardisering vil derfor være viktig.

-Rapport om fysiske, psykiske og sosiale forhold. Første gang skrives denne av fagutviklingssykepleier eller soneleder, og oppfølges så av primærkontakten. Her inngår beskrivelser om førsteinntrykket av pasientens tilstand; fysisk, psykisk, sosialt kontaktnettverk, utgangspunkt for behandling osv. Kan være interessant for

primærleger, men det forutsetter at rapporten er konsis og oppdatert. Gamle opplysninger vil være av mindre betydning for legen.

April 2001: Innspill fra Berit Rosenvinge, alderspsykiatrisk post Åsgård

Berit Rosenvinge, overlege alderspsykiatrisk post/sektoroverlege supraregionalsektor, ønsket å bedre kontakt mellom spesialisttjenesten på Åsgård (psykiatrisk avdeling ved UNN) og hjemmetjeneste / fastlege ved oppfølging av psykiatriske pasienter. Ved å veilede og undervise allmenpraktiker og hjemmetjenestens folk via e-post og web om hva de skal se etter, kunne spesialisttjenesten kanskje hindre unødvendig innleggelser samt ekstra besøk og klargjøring. Hjemmetjenesten og fastlege kan gjøre første vurdering før forspørsel fra fastlege om innleggelse.

Rosenvinge er igang med oppbygging av uteteam fra spesialisthelsetjenesten som kan gjøre egne undersøkelser ute hos pasient. For dem anser hun at e-post kan være nyttig.

Metode ved analyse/ evalueringsforslag

Innspill fra legetjenesten

Legene var aktive omkring forslag på evaluering/analyse. De foreslo audit-skjema istedet for intervju.

Audit-skjemaer (som skal fylles ut etter hver tlf. samtale med hjemmetjenesten) kan for eksempel ha spørsmål:
-Kom telefonsamtalen midt oppe i en konsultasjon?
-Oppfattet du samtalen som relevant?
-Virket telefonsamtalen forstyrrende på påbegynt konsultasjon med pasient?
-Avgjorde telefonsamtalen problemet eller førte det til ny kontakt? (Dette spørsmålet kunne gjentas i forhold til e-post.)

Prosjektet burde også få fram om det ble orden på rutinene i forhold til hjemmetjenesten (for eksempel har ikke hjemmetjenesten i dag en fast tid da de kan nåes på telefon).

Metodevalg

Bakgrunnsopplysninger som bør innhentes ved oppstart:
-ansatte pr yrkesgruppe på legesenter og hjemmetjenester.
-antall brukere ved Stakkevollan og Guleng hjemmetjeneste totalt.
-antall pasienter Nordbyen og Stakkevollan legesentre har til felles med Stakkevollan og Guleng hjemmetjeneste.
-retningslinjer for bruk av e-post mellom legesentre og hjemmetjenester.

Til tross for innspill om kvantitative skjema, bestemte NST at kvalitative gruppeintervjuer om forventninger til e-post løsning og bruk av e-post skal brukes. Dette skyldes at det er få personer i prosjektet slik at kvantitative metoder kanskje ikke vil gi representativ statistikk. Dessuten har det vært lite forskning innenfor området hittil, slik at åpne spørsmål kan være viktig. Legenes innspill kan derimot være en fin tilleggsevaluering på et senere tidspunkt.

Det skal også opprettes et e-post arkiv for hver person som gjennomgåes ved prosjektperiodens slutt. E-post arkivet skal gi svar på:
-Hvor mange e-post meldinger som ble overført.
-I hvilke forbindelser var det e-post ble brukt som kommunikasjonsmiddel.

-Hvilken kommunikasjon som ikke ble gjort med e-post.

Avklaring omkring takstbruk

Takster for telefon- og skriftlig konsultasjon er 1F for allmenpraktikere. Denne kan også brukes for e-post.

Erfaringer med teknologiske løsninger

Lovverkets krav med spesiell relevans til prosjektet (1/6-2001)

Personopplysningsloven (lov av 14. april 2000, nr. 31) trådte i kraft 1.1.2001 [1]. Forskriften til personopplysningsloven ble vedtatt 15.12.2000. I §7-24 står det "Bestemmelsen gir konsesjonsfritak for elektroniske registre og behandlinger av pasientopplysninger. Behandlingene er imidlertid underlagt meldeplikt. Meldeplikten virker bevisstgjørende i forhold til gjeldene regelverk..." [3]

Fra og med 1.1.2001 må derfor ikke helseinstitusjoner lenger søke om konsesjon, men kan nøye seg med meldeplikt. Datatilsynet vil imidlertid drive kontroll for å sikre at forskriftene er overholdt. I "Veiledning i informasjonsikkerhet for kommuner og fylker" [5] fra 1999 er noen av kravene:

a) "..Ved ekstern formidling av sensitive personopplysninger samt informasjon om sikring av slike opplysninger skal data krypteres..". Det er heller ikke likegyldig hvilken kryptering som brukes. Krypteringsalgoritmer som benytter asymmetriske nøkler blir generelt oppfattet som sikrere enn symmetriske. Asymmetriske nøkler er basert på strukturer av offentlige og private nøkkelsystem. Nøklene er elektroniske og opptrer i par, hvorav den ene er offentlig kjent, mens den andre er privat og hemmelig. Fordelen med asymmetriske nøkler er først og fremst at man ikke gir fra seg sin private nøkkel til motpart som skal dekryptere meldingen. Ved bruk av felles (symmetriske) nøkler ved både kryptering og dekryptering, må nøklene overleveres på en sikker måte. Under utveksling over datanettet er det fare for at nøkkelkoden kan fanges opp.

I tillegg bør nøkkellengden være størst mulig for å sikre at inntrengere ikke kan finne fram til rett kode ved å prøve ut alle mulige nøkkelalternativer ("brute force"). Datatilsynet har satt en grense for hvor sterk krypteringen bør være. "Datatilsynet går derfor ut med ny anbefaling, nemlig bruk av krypteringsstyrke tilsvarende "DES128" (112 bits effektiv nøkkel). " skrev Datatilsynet på sine hjemmesider 14.9.01 [5]. DES algoritmen er imidlertid basert på symmetriske nøkler.

b) "..Ingen tjenester skal kunne initieres fra andre soner og inn i sikret sone.."[5]. Datatilsynet opererer med tre begreper: Sikker, intern og ekstern sone. Sikker sone er en sone der sensitiv informasjon slik som pasientopplysninger behandles. Ekstern sone er som regel definert til å være alt utenfor helseinstitusjonens lokaler, i datasammenheng tilsvarer det ikke-avgrensede nettverk som Internett. Intern sone behandler opplysninger som ikke skal eksponeres eksternt, men som heller ikke er definert som sensitive. Kun personer med tilgang til sikret sone får lov til å sende opplysninger ut, slik at ingen utenforstående skal kunne hente opplysninger fra sikret sone etter eget ønske.

c) "..Sikkerhetsrelevante hendelser skal registreres i hendelsesregister.."[5] Datahendelser av sikkerhetsmessig betydning må logges. Dette punktet vil antaglig kunne dekkes gjennom logging som gjøres på servere og i routere/brannmurer i

nettverket, forutsatt at logg gjennomgang gjøres. Alternativt må det installeres tillleggsprogramvare fortrinnsvis i sikret sone for å framskaffe endringslogg, logg for aksesserte filer mm.

d) ”Teknisk sikkerhetsløsning hos bruker skal bidra til å hindre uautorisert utlevering av sensitive personopplysninger ved utilsiktet overføring av data mellom program, eksempelvis ved bruk av ”klipp og lim”-funksjon [5]. Sensitiv e-post må være sikret blant annet med kryptering. Det må heller ikke være fare for at helsepersonell kan feilsende sensitive opplysninger ved uhell. ”..Hovedtyngden av opplysninger som kommer på avveie ved bruk av Internett skyldes ikke bevisste handlinger, men menneskelige feil. Eksempler kan være e-post som sendes til feil adressat og e-postforsendelser med feil vedlegg...” [6].

Sensitiv og ikke-sensitiv e-post må kunne skilles. UNN har fått aksept fra Datatilsynet om at e-post skal kunne benyttes hvis avsender merker e-post med ”ikke sensitiv”, og på den måten går god for at innholdet ikke er sensitivt. Samtidig har UNN en policy om aldri å sende sensitiv informasjon i e-post. Metoden stiller krav til god brukeropplæring og kalles nedklassifisering.

”Nedklassifiseringsprosessen må være en klart definert handling som gir brukeren konkret tilbakemelding på aksjon og konsekvens. Eksempelvis vil vedlegg og innliming fra andre applikasjoner resultere i en aktiv dialog til brukeren om dette er sensitivt.

I tillegg skal systemet nekte nedklassifisering av post med innlimte elementer fra definerte journalsystemer. Det skal også være mulig å definere andre vilkår som gjør det umulig å nedklassifisere [7]. ”

En annen mulighet er to separate nett, ett for sensitive og ett for ikke-sensitive opplysninger. Ved hjelp av terminalservere og tynne klienter kan nettdeling skje uten å måtte doble antall PC’er.

e) Rutiner for tilgang til sensitive opplysninger skal minst kunne omfatte ”..retningslinjer for identifisering og autentisering av medarbeidere..” [5]. Autentisering vil her si å identifisere seg selv mot datanettverket. Autentisering hindrer ikke bare uvedkommende, men kan også fungere som attestering av rette vedkommende (digital signatur).

“Et forhold som Datatilsynet er særlig opptatt av, og som også Statens helsetilsyn har uttalt seg om, er at brukere av Internett i liten grad kan forsikre seg om at mottaker og avsender faktisk er den de utgir seg for å være. For eksempel kan nettstedet til en virksomhet kopieres og gjøres tilgjengelig på en annen Internettadresse. På denne måten kan uvedkommende få tilgang til opplysninger om brukerens høyst private helseforhold - selv om selve overføringen av opplysningene er kryptert.
Problemet med sikker identifikasjon av avsender og mottaker av opplysninger kan imidlertid bli løst ved bruk av digitale signaturer og TTP-tjenester (tiltrodd tredjepart).” [6]

PKI (Public Key Infrastructure) inneholder løsninger for digitale signaturer og tiltrodd tredjepartstjenester.

Public key infrastructure (PKI)
Følgende tekst er i hovedsak hentet fra [7].

PKI er basert på asymmetriske nøkkelstrukturer. Strukturens hensikt er å håndtere nøkler og sertifikater slik at elektroniske transaksjoner kan utføres med tillit mellom aktørene.

Gjennom PKI-teknologi kan en rekke utfordringer med elektronisk kommunikasjon innen helsevesenet tilnærmes. Funksjoner som signering, autentisering og kryptering kan garantere meldingens innhold, avsender og mottager, samt sikre at kun autoriserte får tilgang til ulike informasjonstjenester i nettet.

Kjernen i PKI kan sies å være det digitale sertifikatet og sertifiseringsautoriteten, men innhold og strukturer rundt disse kan variere betydelig.

Digitalt sertifikat og sertifiseringsautoritet (CA)
Et digitalt sertifikat er en datastruktur som inneholder en representasjon av en identitet og tilhørende offentlige nøkkel. Sertifikater kan lagres som filer på harddisk eller diskett, eller legges på fysiske lagringsenheter (for eksempel smartkort).
En person kan ha flere sertifikater, hvor hvert sertifikat kan ha forskjellig bruksområde. Det vanlige er at alle sertifikat låses ned i en fil eller på en lagringsenhet (smartkort). Tilgangen til sertifikatet reguleres av et passord, og som regel åpnes alle nøkler med samme passord. Eventuelt kan passordet erstattes med tilgangssystemer basert på biometri, f.eks. fingeravtrykk.

Sertifiseringsautoritet (eng. akronym: CA) er den som utsteder et sertifikat ved å knytte nøkler til en person/identitet og bekrefter at innholdet i sertifikatet er riktig. Dette gjøres ved at CA signerer sertifikat med sin private nøkkel, og dermed binder et nøkkelpar til en gitt identitet. En CA tilsvarer det som Datatilsynet kaller tiltrodd tredje part, TTP [8].

Tillitsstruktur
En type eksempel på tillitstruktur er om en bedrifts egen CA er ansvarlig for å utstede sertifikater til alle ansatte. Gjennom tillit til én enhet, bedriftens CA, har dermed de ansatte også implisitt tillit til hverandres sertifikater. En felles CA gir et hierarki med der alle stoler på samme CA. Et alternativ til denne organiseringen er et distribuert hierarki der tillit distribueres mellom to eller flere CAer. En slik arkitektur kan bli resultatet når flere virksomheter har sin egen PKI, og disse strukturene ikke springer ut fra samme rot-CA. Prosessen med å sammenkople rot-CAer kalles kryss-sertifisering.

I kombinasjon med begge hierarki-formene kan også en del av oppgavene til en CA settes bort til en RA (Registration Authority – registreringsautoritet). En RA registrerer brukere og bekrefter (fysisk) deres identitet, men vil aldri signere sertifikater.

Motsatt av at alle har tillit til en enhet, er at ingen gitt enhet har tillit, det vil si en brukersentrisk model. Det mest kjente eksemplet er PGP. Her fungerer brukerne som CA ved å signere offentlige nøkler til andre og ved å ha sin egen offentlige nøkkel sertifisert av andre.

Sertifikattyper
Det finnes flere ulike typer sertifikat; X.509, SPKI, PGP, SET og attributtsertifikater. Selv om de likner hverandre, har de likevel forskjellig format og kan ikke brukes om

hverandre. SET og attributtsertifikater er laget for andre formål enn helsevesenets behov, og er derfor uaktuell. PGP mangler tilbakekallingslister, mens SPKI er definert av en arbeidsgruppe fra IETF (Internet Engineering Task Force) som nå er avsluttet uten kjent produktstøtte.

Dermed gjenstår X.509, som finnes i tre forskjellig versjoner. Både den originale X.509v1, definert i 1988, og versjon 2 hadde få muligheter til attributtutvidelser. Versjon 3 har derimot både obligatoriske felt som må fylles ut, felter som normalt er med, og helt valgfrie felt. Algoritmeidentifikasjon, serienummer og den offentlige nøkkelen er eksempler på obligatoriske felter. Eksempler på elementer som normalt legges til, er Certificate Policy utvidelsene og informasjon om bruksområde.[9, 10]

Sertifikatprofiler
I tillegg til forskjellige versjoner av sertifikatet, kan også hver versjon brukes på forskjellige måter. Et eksempel på dette er tidligere nevnte SET, som er en utgave av X.509v3 laget spesielt for sikker e-handel.

En slik tilpasning av en versjon av en standard kalles en profil. Profiler kan defineres av nasjonale eller internasjonale standardiseringsorganisasjoner, av leverandørene selv, eller av store kunder (for eksempel offentlig sektor i Norge). Eksempel på leverandørprofil fins hos Entrust [11]. De har laget en profil, og publisert denne. Mange leverandører følger disse spesifikasjonene. Slike produkter kalles Entrust-Ready produkter.

En annen profil standard er laget av Secured Electronic Information in Society (SEIS). SEIS krever tre nøkkelpar/sertifikater for hver sertifikatinnehaver [9]. Firmaet Smarttrust (eies av Sonera) [12] bruker SEIS, og skal ha implementert støtte for tre nøkkelpar/sertifikater i sine produkter. Zebsigns profil er basert på denne standarden og bruker programvare fra Smarttrust [9,10].

Bruken av nøkkelpar er spesielt sentral i en profil. I helsevesenet og offentlig forvaltning kan det være ønskelig med separate nøkkelpar for signering og kryptering. Slik kan en saksbehandlers krypterte informasjon gjenopprettes gjennom en sikkerhetskopi av krypteringsnøkkel oppbevart av arbeidsgiver. Signaturnøkkelen har ingen tilsvarende sikkerhetskopi, og signaturens validitet må dermed ikke samtidig kompromitteres. Dette støttes av både Entrust og SEIS, mens nøkkelbruken for autentisering er ulik.

Zebsigns PKI løsning
ZebSign AS [13] er en norsk CA som ble etablert mars 2001. Eierne av Zebsign er Telenor og Posten i fellesskap som dermed har fusjonert sine PKI løsninger. I mai 2001 fikk NH prøve ut GemPC410 smartkort og smartkortholder fra Smarttrust. Zebsign forhandler PKI-løsningen.

Smarttrust sin løsning benytter Secure Socket Layer (SSL) med RSA protokoll for kryptering og digitale signaturer sammen med X.509 sertifikater. Løsningen er tilpasset PKCS # 11 v 2.01, en standard for tilkopling til identifikasjon (tokens) som for eksempel smartkort.

SSL
Følgende tekst er basert på [14]:

SSL er en portokoll laget av Netscape Communication Corporation for å sikre toveis kommunikasjon. SSL brukes vanligvis sammen med internett-teknologi, for eksempel i Microsoft Internet Explorer og browsere fra Netscape. SSL kan initieres av bruker ved å erstatte URL prefix ”http:” med ”https:” i browser. All HTTP informasjon krypteres, også URL adresser og og påloggingsinformasjon. SSL ved kryptering i browser synliggjøres i Netscape gjennom et ikon av en stor nøkkel nederst i venstre hjørne hvis 128-bits kryptering brukes, et ikon med liten nøkkel hvis 40-bits nøkkel benyttes og en brukket nøkkel hvis kryptering mangler. I Explorer vises en lås nederst i venstre hjørne hvis et dokument ble nedlastet med SSL. Eksempler på andre protokoller som SSL kan sikre er post-forsendelse og mottak (smtp, POP3 og IMAP), nyhetsgrupper (nntp, Usenet news) og katalogtjenester (LDAP).

SSL består i praksis av to lag, et meldingslag over et monitoreringslag som igjen ligger over data-transportlaget i IP modellen (fig 1). Over meldingslaget ligger applikasjonslaget (for eksempel HTTP).

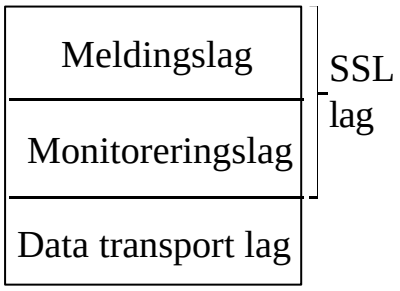


Fig. 1. SSL-lagene i IP-modellen.

Monitoreringslaget sender blokker av data mellom klient og server, og tilbyr sikkerhet til øvre SSL-lag hvis protokoller her må reforhandles. Meldingslaget selv forhandler om bruk av sikkerhetsprotokoller og utveksling av informasjon.

SSL 3.0 tilbyr kryptering gjennom RC4 med 40 og 128-bits nøkler, evenuelt DES, DES40, 3DES_EDE, RC2, Idea og Fortezza. Integritet tilbys gjennom spesifikke hash-funksjoner som MD5 (128-bits) og SHA (160-bit) [15]. Autentisering gjøres gjennom X.509 v1, v2 eller v3 sertifikat og ikke-benekting gjennom kryptografisk signering med for eksempel RSA eller Diffie-Hellman. I tillegg tilbys komprimering før kryptering.

RSA
RSA er en asymmetrisk krypteringsalgoritme utviklet i 1997 av Ronald Rivest, Adi Shamir og Leonard Adleman. Algoritmen kan brukes både for informasjonskryptering og som basis for digiale signaturer/autentisering. Nøkkellengden til algoritmen kan variere. USA har imidlertid fram til januar 2000 hatt restriksjoner på eksport av krypteringsalogritmer av forsvarshensyn. Derfor har RSA-moduler med krypteringsnøkler av størrelse over 512 bits blitt nektet eksportert (samt alle symmetriske krypteringsalgoritmer over 56 bits). I dag kan krypteringsalgoritmer eksporteres uten lisens med mindre mottaker er et annet lands statsmakt eller land USA har handelsforbud imot. Eksport til at annet lands statsmakt kan godkjennes under lisenskontroll. [16]

PKCS #11
Public Key Cryptography Standardene (PKCS) er standarder spesifisert av RSA Laboratories og partnere for å styrke utviklingen av asymmetrisk kryptografi. De første

standardene ble publisert i 1991, og har blitt innspill i utviklingen av en rekke standarder som blant annet SSL.

PKCS #11 er standard for tilkopling av identifikasjon (token) som for eksempel smartkort. Standarden definerer et programmeringsgrensesnitt (API) kalt Cryptoki som inneholder kryptografisk informasjon og utfører kryptografiske funksjoner. Det tar seg blant annet av ressursdeling og å gi applikasjonen et enhetlig bilde av identifikasjonen. Cryptoki er en forkortelse for cryptograpgic token interface. [17]

Public key infrastructure i forhold til krav fra Datatilsynet

Hvert legesenter og hjemmetjeneste vil måtte gjennomføre sin egen risikoanalyse. Risikoanalysen må sees i forhold til krav fra Datatilsynet. I matrisen under forutsettes det at rutiner omkring PKI for tildeling, lagring og tilbakekalling av sertifikater og nøkler er ordnet på en sikkerhetsmessig forsvarlig måte av enten NH eller en annen tiltrodd tredjepart.

Krav fra Datatilsynet	**PKI med Internett-tilknytning**
a) Kryptering	Ja, forutsatt at PKI-løsning har sterk nok kryptering.
b) Ingen tjenester initiert inn mot sikret sone	PKI muliggjør ende-til-ende kryptering, men hvis postserver står på intern sone istedet for sikret sone vil all post selv internt på helseinstitusjonen måtte krypteres med PKI. Dette betyr blant annet at man ikke kan gjøre bruk av virusbeskyttelse på postserver men er avhengig av oppdaterte virusprogrammer på hver klient. Bruk av PKI vil også være ressurskrevende for nett og maskiner.
c) Tilstrekkelig logging	PKI server sammen med routere, brannmur og andre servere vil tilsammen antaglig kunne skaffe nok logging, forutsatt at rutiner for kontroll av logg fungerer. Alternativt må det fortrinnsvis på sikker sone installeres tillleggsprogramvare for å framskaffe endringslogg og logg for aksesserte filer mm.
d) ”klipp-og-lim” mulig?	Det vil være umulig/svært vanskelig å hindre ”klipp-og-lim” fra pasientjournal direkte inn i en e-post klient som kjører på lokal maskin (f.eks. Hotmail eller Outlook). Hvis Internett tillates, må mulighetene for at helsepersonell gjennomfører utilsiktet utlevering være små (lav risiko). Bruk av to helt forskjellige e-post klienter uten felles adressebok vil kanskje være en mulighet, forutsatt at det finnes bevisstgjørende opplæringsrutiner for brukerne.
e) Entydig identifisering av sender og mottaker	Ja, forutsatt at PKI har gode nok signerings- og autentiseringsmekanismer.

Terminalserver/tynne klienter

En terminalserver er karakterisert ved at ingen programmer eller data overføres til klienten annet enn skjermoppdatering og utskriftsdata. Terminalserveren utfører alle programmer og behandler data på vegne av klienten.

Tynn klient kalles en applikasjon som utfører kommunikasjon mot en terminalserver. Klienten formidler informasjon fra tastatur og mus, og mottar oppdaterte skjermbilder og utskriftsdata fra terminalserveren.

Kravene på klientsiden er små, både når det gjelder maskinvare og programvare som må til for den grafiske forbindelsen, derav navnet tynne klienter. Tynne klienter er ikke et nytt fenomen. Konseptet har eksistert i flere år for arbeidstasjoner (f.eks. X-terminaler) [18]. Tynne klienter er ikke bare interessant for å kunne utnytte eldre PC'er og forenkle driftsoppgaver, men minst like aktuelt fordi serveradministrator kan kontrollere klientenes rettigheter. For eksempel er det mulig å sperre bruk av "klipp og lim"-funksjon mellom applikasjoner på terminalserver og klient. Bruker ville dermed ikke kunne klippe fra pasientjournalen og sende denne til feil e-post adresse.

De fire mest aktuelle terminalserver løsningene er Windows NT server 4.0 Terminal Server Edition og Windows 2000 Terminal Services som begge støtter Microsoft Remote Desktop Protocol (RDP) og Citrix MetaFrame eller Citrix XP som bruker Citrix Independent Computing Architecture (ICA) protocol og SSL [19]. Begge Citrix produktene må installeres over et av Windows produktene.

RDP

Remote Desktop Protocol (RDP) er en protokoll som er basert på T.120 protokollfamilien definert av International Telecommunications Union (ITU). Det er RDP som gir mulighet for scrolling av et dokument på server ettersom server sender skjermoppdateringer til klient. Tastatur og musbevegelser overføres også via RDP protokollen. RDP kjører mellom data transport laget (TCP) og applikasjonslaget i IP-protokollen. Både kryptering, inn- og utpakking av data, kanalvalg og pakkeinndeling blir gjort i RDP.[20] Hvis kryptering ikke brukes ved overføring, kan datapakker som overføres fanges opp. RDP standarden som Microsoft bruker er dokumentert, men ikke sikkerhetsrutinene i protokollen [21].

RDP 5.0 i Windows 2000 Terminal Services bruker RC4 kryptering med enten lav, medium eller høy grad av sikkerhet. Lav grad av sikkerhet vil si 56-bits (eller 40 mot eldre klienter) kun fra klient til server (for beskyttelse av passord overføring ved pålogging), medium vil si 56-bits kryptering begge veier. Høy grad av sikkerhet vil si 128-bits kryptering begge veier (i Norge etter januar 2000). Det er også mulig å benytte IPsec for enkapsulering av RDP data.[22]

Secure ICA

Citrix' Independent Computing Architecture (ICA) kan brukes sammen med Windows NT server 4.0 Terminal Server Edition og Windows 2000 Terminal Services, men passer også sammen med mange andre operativsystemer både som server og som klient. ICA løsningen hadde en del funksjonalitet som ikke fantes for RDP 4.0 (brukt i Windows NT server 4.0 Terminal Server Edition), men som er tilkommet i RDP 5.0 (Windows 2000 Terminal Services), blant annet mulighet for "klipp-og-lim" mellom klient og serverapplikasjon og bruk av browserklient [23]. I seg selv har ikke ICA sikkerhetsstøtte.

Med Citrix Metaframe 1.8 ble Secure ICA en standard. Secure ICA tilbyr RC5 for å kryptere pakker, bruker 64 bits blokkstørrelse, tolv runder (antallet runder krypteringen anvendes på hver blokk)og 40, 56, eller128 bits nøkkellengde [24]. I likhet med RDP og SSL implementeres Secure ICA i to lag mellom applikasjonslaget og data transport laget i IP-modellen. I den nyeste terminalserver applikasjonen Citrix XP har man også

mulighet for å bruke webbrowser som interface på klient. Secure ICA byttes da med SSL, blant annet for å kunne benytte HTTPS-porten gjennom brannmurer, og dermed unngå at flere porter enn nødvendig blir stående åpne for trafikk.

Terminalserver/ tynne klienter i forhold til krav fra Datatilsynet

Krav fra Datatil-synet	**Terminalserver/tynne klienter med Internett tilknytning**
a) Kryptering	Ja, forutsatt sterk nok kryptering.
b) Ingen tjenester initiert inn mot sikret sone	Man kan tenke seg et oppsett der klient får tilgang til journal/sensitiv informasjon via en terminalserver og e-post og webtilgang til Internett kjøres via en annen. Klienter kan nektes "klipp-og-lim" mellom sikker og ekstern sone i terminalserveroppsett.
c) Tilstrekkelig logging	Terminalserver sammen med routere, brannmur og andre servere vil tilsammen antaglig kunne skaffe nok logging, forutsatt at rutiner for kontroll av logg fungerer. Ev. må det fortrinnsvis på sikker sone installeres tillleggsprogramvare for å framskaffe endringslogg og logg for aksesserte filer mm.
d) "klipp-og-lim" mulig?	Mulighet for "klipp-og-lim" kan sperres på terminalserver.
e) Entydig identifisering av sender og mottaker	Må gjøres gjennom påloggingsrutiner på terminalserver. Identifisering av avsender på e-post vil gjøres i henhold til påloggingsrutiner på e-post klient. Dette er i utgangpunktet basert på statiske påloggingsrutiner uten hardware identifikasjon. Bruk av sterk PKI vil kunne øke sikkerheten ytterligere.

DORIS

DORIS er et multimediasystem for bruk i telemedisinske tjenester, utviklet for helsevesenet av NST og Well Diagnostics. All informasjon i DORIS er lagret i en ordentlig database, noe som gir sikkerhet i forhold til separate brukerkonti der rettighetene kan begrenses og kontrolleres. I tillegg er det mulighet for å logge all aktivitet [25].

DORIS benytter innebygget kryptering med bruk av private nøkler på inntil 448-bits over Blowfish algoritmen [7]. Blowfish er en symmetrisk blokk-algoritme, og baserer seg på en hemmelig nøkkel som må overleveres [14]. Det ble i 1995 utlyst en konkurranse for å se om noen kunne knekke koden. Noen varianter av Blowfish-algoritmen ble knekket, mens andre varianter anses forsatt som sikre. [26]

I tillegg har DORIS i det siste også hatt mulighet for å benytte Rijndal-algoritmen ved overføring. Denne algoritmen har status som Advanced Encryption Standard (AES) [27].

I DORIS defineres brukere og brukeres e-post adresser i egen adressebok. Denne adresseboken brukes så med standard ved overføring. DORIS vil derfor skille sensitiv e-post fra vanlig e-post ved bruk av et annet grensesnitt og en egen adressebok."Klipp-og-

lim" sperres ikke ved bruk av DORIS, men sjansene for utilsiktet feilutlevering av sensitiv informasjon blir betydelig redusert.

DORIS i forhold til krav fra Datatilsynet

Krav fra Datatilsynet	**DORIS med Internett-tilknytning**
a) Kryptering	Blowfish-algoritmen og måten de symmertiske nøklene overleveres på, må eventuelt undersøkes nærmere. Hvis dette ikke er tilstrekkelig, kan kryptering med IPsec i routere innføres eller enda bedre en sterk PKI løsning som vil gi ende-til-ende kryptering.
b) Ingen tjenester initiert inn mot sikret sone	Forutsetter at postserver enten står på sikker sone eller at klient henter post fra intern sone og denne posten er kryptert inn til klient.
c) Tilstrekkelig logging	DORIS sammen med routere, brannmur og andre servere vil tilsammen antaglig kunne gi nødvendig logg, forutsatt at rutiner for kontroll av logg fungerer. Ev. må det installeres tillleggsprogramvare for å framskaffe endringslogg og logg for aksesserte filer mm. fortrinnsvis inne på sikker sone.
d) "klipp-og-lim" mulig?	Ja, men risiko for utilsiktet utlevering hos helsepersonell vil reduseres kraftig hvis sensitiv e-post og ikke sensitiv e-post skilles i to forskjellige applikasjoner som ikke ser like ut. Det er mulighet for å sende til feil e-post adresse gjennom DORIS, men det vil å så fall komme til helsepersonell med taushetsplikt hvis adressebok er rett satt opp.
e) Entydig identifisering av sender og mottaker	DORIS tilfører ekstra sikkerhet ved at bruker har eget passord ved pålogging av DORIS. Likevel er autentisering i utgangspunktet basert på statiske rutiner uten hardware-identifikasjon. DORIS med sterk PKI ville kunne forbedre sikkerheten ytterligere.

Hvorfor passet ingen av sikkerhetsløsningene våre behov?

Til tross for at Datatilsynet fronter sikkerhet gjennom bruk av terminalservere og tynne klienter medfører slike løsninger endel ulemper. En av disse ulempene er at å stenge for "klipp-og-lim" funksjon vil også vanskeliggjøre utbygging av kontakt direkte ut mot pasienter i framtidige NH prosjekt. Kontakt mot nye (og dermed ikke identifierte pasienter) vil måtte foregå direkte over Internett. Å ivareta disse pasientene samtidig som man har et sikkert helsenett blir en stor framtidig utfordring.

Standardene som brukes ved terminalserver/tynne klienter er til dels udokumenterte og de største produsentene har ennå ikke samlet seg om en felles standard. RDP standarden som Microsoft bruker er dokumentert, men ikke sikkerhetsrutinene i protokollen. Secure ICA protokollen mangler også dokumentasjon. Det finnes imidlertid alternative terminalserverteknologier for Unix systemer. X, XDMCP, VWC og RFB protokollen gir mulighet for terminalserving, men med varierende grad av sikkerhet og ofte mindre funksjonalitet [21] . NH er også bygget opp omkring en nettverksstruktur basert på flere sikkerhetsbarrierer ut mot Internett, som kan stå i motsetning til terminalservere. Det ville bli ressurskrevende å legge om hele nettet til terminalservere, en løsning som i

tillegg ser ut til å vanskeliggjøre videre utbygging av tjenestetilbud i helsenettet på flere felt.

Innenfor PKI løsninger viste det seg at standarder og utvikling ikke har kommet så langt som vi hadde håpet på. Det er fortsatt problemer med utveksling av sertifikater. Det er også usikkert om profiler fra en CA som arbeider med flere fagbransjer vil gi optimal sikkerhet i helsenett. For eksempel vil det kunne være ønskelig at sertifikatet kan definere en persons rolle innen helsevesenet entydig (yrke, institusjon, avdeling osv). NH er igang med å se på mulighetene for å danne egen CA for helsevesenet.

Med DORIS som løsning må Blowfish eller Rijndael benyttes ende-til-ende hvis e-post server skal stå på intern sone. Denne løsningen ble det ikke arbeidet mye med før nedleggelse av prosjektet.

Relaterte prosjekter og et høringsutkast

SESAM-prosjektet gjorde bruk av PKI for sikker overføring mellom Bjerke hjemmetjeneste og Aker sykehus. Sertifikatene var levert av Telenor og tilpasset Entrust applikasjonene og Telenors TTP-tjeneste. Rapport i prosjektet kom i februar 2001 [2]. Svært mange av problemstillingene her er aktuelle for Nordmail, samtidig som tilgang til Internett ikke var en del av prosjektet.

"Forprosjekt for PKI i helsenett" er et forprosjekt som pågår høsthalvåret 2001. Det er igangsatt av SHD under programmet Nasjonalt Helsenett. KITH har prosjektledelsen og utfører prosjektet sammen med NST, SHD, Rikstrygdeverket, Statens helsetilsyn og Statens autorisasjonskontroll for helsepersonell. Problemstillinger fra Nordmail blir diskutert i dette prosjektet.

Prosjektet Elvira ble igangsatt av NST med deltagelse fra KITH, Universitetet i Tromsø og Telenor FoU. Hoveddelen av prosjektet ble avsluttet i april 2001, mens spredningsaktivitet gjennom publisering pågår ut 2001 [28]. Elvira hadde som målsetning å foreta innledende vurderinger av mulighetene for å utvikle og implementere et system for nettbasert tilgang til pasientinformasjon. Visjonen var at autorisert helsepersonell skal få tilgang til all nødvendig helseinformasjon i møte med pasienter. Erfaringer og problemstillinger fra hospitering i Nordmail ble gitt som innspill til Elvira.

Prosjektet "elektronisk samhandling i pleie og omsorg" initieres nå ved NST etter ønske fra SHD om kartlegging av de viktigste meldingsutvekslingene mellom pleie og omsorgstjenesten og de andre helsetjenestene. Et av resultatene fra prosjektet skal være kost/nytte-vurderinger. Rutiner og kjennskap til førstelinjetjenesten samt kontakter i Tromsø kommune fra Nordmail vil bli videreført i prosjektet.

Et prosjekt omkring sikkerhet med Thales og NST som partnere ble våren 2001 tildelt midler fra Forskningsrådets MUNIN program. Prosjektet arbeider med sikkerhetsproblemstillinger innen helsevesenet, blant annet gjennom å tilby løsninger for sikret e-post kommunikasjon. Erfaringene og problemstillingene innen datasikkerhet fra Nordmail vil dermed videreføres.

28/09-2001 sendte Arbeids- og administrasjonsdepartementet ut "Høring –utkast til forskrift om elektronisk kommunikasjon med og i forvaltningen" [29]. Her gis utkast til krav og forslag som omhandler mottak av elektroniske henvendelser,

virksomhetssertifikater, sikring av signaturfremstillingsdata og dekrypteringsdata ved bruk av virksomhetssertifikat. NST ble bedt om å komme med innspill til høringen.

Hva gjorde vi rett?

NST fikk kjennskap til hvordan hjemmetjenesten og allmenpraktikerne arbeider. Hospitering var en fin måte å komme i kontakt med prosjektets nøkkelpersoner på og å få kunnskap om deres hverdag. Når helsepersonell kun gjenforteller, er det en fare for at de utelater hendelser og omgivelser som taes for gitt.

Erfaringene vil være nyttig ved utvikling av telemedisin i førstelinjetjenesten. Sosial- og helsedepartementet har vist interesse for prosjekter omkring kommunikasjon innen førstelinjetjenesten og har fulgt med på Nordmail prosjektet. Innspill fra behov som kom fram gjennom hospitering og arbeid med sikkerhetsløsninger vil bli videreført (se forrige avsnitt).

Det er utvilsomt et stort behov for overføring av tekstbasert informasjon innen helsevesenet, noe som blant annet beskrives i Sosial- og helsedepartementets plan "Si @!" [30]. Samtidig gir tekstbasert informasjon store utfordringer for helsevesenet, blant annet fordi den i dag er ustandardisert og krever mange avklaringer omkring sikkerhet og innsyn. Prosjektet hadde muligheter for ytterligere styrking gjennom involvering fra spesialisthelsetjenesten (jfr. innspill fra Berit Rosenvinge).

Teknologisk fikk NH og NST brynt seg på en del viktige problemstillinger innen sikkerhet. Resultatene fra denne prosessen er blant annet en nesten ferdig mal for sikkerhetshåndbok for små helseinstitusjoner tilknyttet NH (se vedlegg 2). Ifra 1. januar 2001 har det vært påkrevet for små helseinstitusjoner å ha egnet sikkerhetstrategi og –policy [31]. Det har vært forespørsler om håndboken også fra andre regionale helsenett.

Hva burde vært gjort anderledes?

I ettertid har prosjektet blitt forvansket ved at mange strukturer var i forandring samtidig som prosjektet dro ut i langdrag. Sikkerhetsrådgiver var ikke på plass på NST da prosjektet ble igangsatt, NH ble skilt ut fra NST som et fylkeskommunalt foretak, utskiftninger skjedde på brukersiden, lovverket og dermed krav fra Datatilsynet var i endring osv. Noen forandringer var umulige å forutse før prosjektstart. Men først og fremst burde mulighetene for å komme i mål teknologisk vært sjekket bedre ut før prosjektoppstart. Det ville i stor grad ha kompensert for andre endringer. PKI og andre sikkerhetsløsninger viste seg å være langt mindre standardisert og ferdige enn antatt. Prosjektet har også slitt under mangel på tilførte ressurser, først og fremst i form av personell.

Prosjektet ble tungrodd fordi alle parter må kontaktes separat, og det har vært liten mulighet for å samkjøre informasjonsmøter, oppdateringstelefoner o.l. Selv om Nordmail møtte en svært positiv innstilling hos alle involverte, tok informasjonsarbeidet tid. Nødvendigheten av å oppdatere prosjektdeltagere samtidig som arbeidet med å finne en akseptabel teknisk løsning pågikk, var hovedårsak til prosjektnedleggelse.

Konklusjon

Overføring av tekstbasert informasjon mellom helseinstitusjoner vil være viktig for bedre samhandling innen helsevesenet i fremtiden. Nordmail gav ikke NST noen

avklaring på hvor nyttig e-post kan være mellom hjemmetjenesten og primærlege, men problemstillinger og prinsippløsninger som er blitt arbeidet fram vil være nyttige. NST vil videreføre disse i andre prosjekter.

Når Nordmail prosjektet ikke ble gjennomført skyldes dette fortsatt uavklarte spørsmål omkring datasikkerhet i forhold til lovverket. Nordmail ble så forsinket i tid at NST fant det nødvendig å avslutte prosjektet av hensyn til brukerne.

Referanser

1. Arbeids- og administrasjonsdepartementet. *Lov om pasientrettigheter (personopplysningsloven).* http://www.lovdata.no/all/hl-20000414-031.html [30.11.01]
2. KITH. *SESAM. Sikker elektronisk samhandling på Aker sykehus. Bruk av digitale signaturer og offentlig nøkkelkryptografi.* KITH Rapport 4/01
3. Arbeids- og administrasjonsdepartementet. *Forskrift til personopplysningsloven.* http://www.lovdata.no/for/sf/aa/aa-20001215-1265.html [30.11.01]
4. Datatilsynet. *Veiledning i informasjonssikkerhet for kommuner og fylker.* Mars 1999. TV-202:1999
5. Datatilsynet: *Sterkere kryptering er nødvendig* http://www.datatilsynet.no/infosik/tema/krypto/kryptering.html [30.11.01]
6. Datatilsynet. *Helsepersonell og Internett* http://www.datatilsynet.no/arkiv/infoskriv/helsepersonell/ji003.html [30.11.01]
7. Løvold A. *Sikkerhetsmodul i IKT-baserte pasienttjenester*. http://www.telemed.no/publikasjoner/nedlastbare/pki_nst_rap.pdf [30.11.01]
8. Zebsign AS. *Tiltrodd tredjepart.* http://peid.sds.no/prod/teknologi.htm#Tiltrodd [30.11.01]
9. Adams C, Lloyd S. *Understanding public-Key Infrastructure*. Indianapolis, USA, Macmillan Technical Publishing
10. JB Consult. *Elektroniske ID-kort*. http://www.statskonsult.no/prosjekt/pki/rapporter/elektronisk%ID.pdf [30.11.01]
11. Entrust. http://www.entrust.com [30.11.01]
12. Smarttrust. http://www.smarttrust.com [30.11.01]
13. Zebsign AS. http://www.zebsign.com [30.11.01]
14. Garfinkel S, Spafford G. *Web security & Commerce*. USA, O'Reilly & Associates
15. Hirch FJ. Introducing SSL and Certificates using SSLeay http://www.ultranet.com/~fhirsch/Papers/wwwj/article.html [30.11.01]
16. RSA Security. *United States Cryptography Export/Import Laws* http://www.rsasecurity.com/rsalabs/faq/6-4.html [30.11.01]
17. RSA Security. *RSA Laboratories PKCS #11 - Cryptographic Token Interface Standard* http://www.rsasecurity.com/rsalabs/pkcs/pkcs-11/index.html [30.11.01]
18. Hansen O. *Tynne klienter og trådløse nett. Et samarbeidsprosjekt mellom Institutt for elektronikk og Avdeling for teknologi ved Høyskolen i Sør-Trøndelag.* http://venus.iet.hist.no/rapport/hoved.html [30.11.01]
19. Microsoft. RDP & Citrix ICA Feature Overview http://www.microsoft.com/windows2000/server/evaluation/features/rdp.asp [30.11.01]
20. Microsoft. Remote Desktop Protocol in Windows CE Platform Builder 3.0 http://www.microsoft.com/windows/embedded/ce/evaluation/features/indepth/rdpinpb30.asp [30.11.01]
21. Schmidt M. *Protocol Analysis* http://www.nue.et-inf.uni-siegen.de/~schmidt/tcsecurity/protocols.html [30.11.01]

22. Security Administrator. Terminal Services, part 4
http://www.secadministrator.com/Articles/Print.cfm?ArticleID=20288 [30.11.01]
23. Virtual Network Computing. http://www.uk.research.att.com/vnc/ [30.11.01]
24. East Coast Computer Inc. *Citrix Secure ICA technical overview*
http://ecc400.com/citrix/seci5my5.htm [30.11.01]
25. Well Diagnostics. *Specification DORIS professional.*
http://www.welldiagnostics.com/en/specification_dp3.pdf [30.11.01]
26. Christoyannis C. *Blowfish*
http://www.hack.gr/users/dij/crypto/overview/otherbc.html [30.11.01]
27. Computer Security Research Center. *AES algorithm (Rinjndael) Information.*
http://csrc.nist.gov/encryption/aes/rijndael/ [30.11.01]
28. Bellika JG, Andreassen H, Bergmo TS, Christiansen E, Hartvigsen G, Hartviksen G, et.al. *Nettbasert pasientinformasjonssystem. Hovedrapport fra Elviraprosjektet*
http://www.telemed.no/publikasjoner/nedlastbare/elvira_hovedrapp.pdf [30.11.01]
29. Arbeids- og administrasjonsdepartementet. *Høring –utkast til forskrift om elektronisk kommunikasjon med og i forvaltningen*.
http://www.odin.dep.no/aad/norsk/publ/hoeringsnotater/002061-990018/index-dok000-b-n-a.html [30.11.01]
30. SHD. *Elektronisk samhandling i helse- og sosialsektoren. "Si @!"*
http://odin.dep.no/shd/norsk/publ/handlingsplaner/030011-120002/index-dok000-b-n-a.html [30.11.01]
31. Datatilsynet. *Fra sikkerhetsgodkjenning til meldeplikt.*
http://www.datatilsynet.no/infosik/informasjon/SI-800_00.pdf [30.11.01]

Vedlegg

Vedlegg 1: Protokoll
Vedlegg 2: Utkast til sikkerhetshåndok for små helseinstitusjoner.

PROTOKOLL

Nord-mail

Oppnås bedre koordinasjon og kommunikasjon mellom hjemmetjeneste og fastlege ved bruk av PKI-sikret e-mail?

Dato: 31.12.01

Prosjektleder:
Siri Uldal, (siv. ing. fysikk)
Nasjonalt senter for telemedisin
Regionsykehuset i Tromsø
Pb 35
9038 Tromsø

Studiekomite /kontaktpersoner for undersøkelsen:

Unni Ringberg, Nordbyen legesenter
Trond Brattland, Stakkevollan legesenter
Else Thorill Nielsen, Stakkevollan hjemmetjeneste
Elisabeth Sausjord, Guleng hjemmetjeneste
Hege Andreassen, Nasjonalt senter for telemedisin
Jan Norum, Nasjonalt senter for telemedisin
Siri Birgitte Uldal, Nasjonalt senter for telemedisin

Områdeleder og PRO-sjef i Tromsø kommune er informert om prosjektet.

Sammendrag

En uformell forundersøkelse viste at personell ved Stakkevollan og Guleng hjemmetjenester i Tromsø opplever en svært travel hverdag. Det samme gjelder personell ved Nordbyen og Stakkevollan legesenter, som til enhver tid har ca 20-40 felles pasienter med hjemmetjenestene. God samhandling er av betydning for pasientene. I dag er dette vanskeliggjort bl.a. fordi fastlege og hjemmetjeneste ikke har noen "faste møteplasser". Hjemmetjenestens folk ringer derfor av og til når det er pasienter tilstede inne hos legen. Da har legen dårlig tid og må gi raske svar som sjelden kan kvalitetssikres ved oppslag i journal. Hjemmesykepleierne opplever usikkerhet omkring medisindosene når denne kun er angitt muntlig over telefon. Den skriftlige kommunikasjon kommer ofte sent fram. Mangel på kontakt mellom helsearbeidere øker faren for at pasientene kan få forverret sin sykdomstilstand grunnet feilbehandling.

Prosjektets mål er å undersøke om kommunikasjon og koordinasjon mellom hjemmetjeneste og fastlege kan bedres ved bruk av elektronisk post. Denne posten skal være sikret mot innsyn fra uvedkommende (kryptering), beskyttet mot endring underveis (kontrollmelding) og attestert av rette vedkommende (digital signatur). Prosjektdeltagerne vil bli koplet til Nord-Norsk Helsenett (NH); et internt fagnettverk for helsearbeidere i Nordland, Troms og Finnmark. Det er også planlagt at både allmenpraktikerne og hjemmetjenesten får tilgang til oppkopling mot norske fagnettverk.

INNHOLD

Introduksjon

Hjemmetjenesten ivaretar mennesker med sammensatte behov for omsorgs- og helsetjenester. Regelmessig samarbeid mellom legetjeneste og hjemmesykepleie er viktig med hensyn til forebygging, diagnostisering, behandling og oppfølging av sykdom. Sviktende samarbeid kan gjøre pasientene skadelidende [1]. For eksempel kan diagnostisering av aldersdemens være vanskelig for primærlegen som kun møter den eldre pasienten på sitt kontor. Her kan hjemmesykepleien ha data om pasientens funksjonsevne/funksjonstap som bidrar til et bedre vurderingsgrunnlag [2,3]. Den psykiatriske pasient kan også være vanskelig å diagnostisere for legen uten grunnlagsopplysninger fra hjemmesykepleien. For sterkt funksjonshemmede mennesker, multihemmede og lignende gjelder det samme. Samtidig har legen det medisinske ansvaret [2,3]. Det er derfor nødvendig med en koordinert innsats fra flere yrkesgrupper innen omsorgstjenesten (PRO) og legetjenesten. I "Rundskriv om kvalitet i pleie- og omsorgstjeneste" fra Statens Helsetilsyn [4] heter det:

"..Organisatoriske forhold må ikke være til hinder for et strukturert tverrfaglig samarbeid og nødvendig informasjonsflyt mellom faggrupper. Det bør foreligge faste samarbeidsrutiner mellom lege og hjemmesykepleie og med den fylkeskommunale tannlegetjenesten som omfatter kontakt gjennom telefon, møter, o.l..."

Ifølge en forundersøkelse blir i dag beskjeder mellom Nordbyen og Stakkevollan legesentre og Guleng og Stakkevollan hjemmetjenester som oftest gitt via telefon eller pr. brev. Forsendelse og postgangen tar tid; informasjonen kan komme fram etter 1-2 dager hvis legesenteret/hjemmetjeneste sender den ut med en gang. Telefon krever at begge parter er tilstede samtidig. Tilbakeringing blir derfor ofte nødvendig. Telefonen oppfattes derfor ikke alltid som et egnet kommunikasjonsredskap.

Forundersøksøkelsen bestod i en hospitering på Stakkevollan og Guleng hjemmetjeneste samt Nordbyen legesenter i til sammen 1 ½ dag. Hospiteringen sammen med oppfølgende samtaler og diskusjoner siden, viste at hverdagsrutinene i alle institusjonene er svært hektiske. Både legetjenesten og hjemmetjenesten starter dagen med morgenmøter fra kl. 8.00 til ca 8.30. Hjemmetjenesten følger deretter opp brukerne sine ute. De opplever at mangel av mobiltelefoner gjør det vanskelig å nå alle ansatte ute i felten. Imellom visittprogram er det kjøring/ gåing/bruk av offentlig transport mellom brukere. Hjemmetjenesten prøver å unngå å bruke brukernes telefoner. På legesentrene forsøker legene så tidlig som mulig å komme igang med pasienter etter morgenmøtet. I tillegg til dagens timelister, får de ofte inn pasienter akutt (som t.o.m. overskrider konsultasjonstidene avsatt til akutte formål). Endel av pasientene kommer med psykiske lidelser eller underlivsproblemer; noe som gjør det ekstra vanskelig for lege og ubehagelig for pasient å bli avbrutt. Legesekretærene tar blodprøver, EKG og overfører prøver til lab på RiTø i tillegg til innringinger for timebooking, reseptordning mm. På toppen kommer dokumentasjons- og papirarbeide. Matpausene blir hastige både på legesenter og hjemmetjenesten, og brukes gjerne til å oppdatere seg på kollegers arbeide. I tillegg er det et ønske fra begge parter om å skjerme lunsjene. Legene er sjelden tilgjengelige etter lunsj før i en kort periode etter kl. 15.00, mens dagvaktene ved hjemmetjenesten da avslutter etter et kort oppsummeringsmøte. Forundersøkelsen vitner om stort tidspress, i motsetning til artikler som gjerne fokuserer på kulturforskjeller mellom hjemmesykepleiere og lege, som forklaring på hvorfor kommunikasjonen er vanskelig eller fungerer dårlig [2,3,5]. Dette prosjektet vil ikke fokusere på kulturforskjeller, men ha holdningen at disse må respekteres, samtidig som de ikke får ødelegge for et godt samarbeid.

Norske leger har begynt å ta i bruk internettjenester. Først og fremst brukes Internett i fagnettverk og faglig utvikling, men også til pasientkommunikasjon [6]. Såvidt vi vet, har ikke bruk av e-mail mellom hjemmetjeneste og primærlege vært gjenstand for undersøkelser. Det er derfor interessant å vurdere bruken av e-mail som kommunikasjonsmiddel i denne sammenheng.

NST begrunner interesse for e-mail oppkopling mellom hjemmetjeneste og primærlege med:

1. E-mail i klinisk bruk har fått positiv omtale [7,8] bl.a. fordi man ikke er avhengig av at den annen part er tilstede. Lege- og hjemmetjeneste kan tilpasse kontakt til andre gjøremål, og dermed redusere avbrudd på ugunstige tidpunkt. F.eks. ble det nevnt i forundersøkelsen at legene kanskje da kan få bedre tid til å slå opp i pasientens journal.

2. En undersøkelse har vist at e-mail var nyttig for strukturering av tanker hos pasienter som sendte e-post til sin psykolog [9,10]. Samtidig har mangel på nøyaktig og etterspurt informasjon mellom helsepersonell vært nevnt som et problemområde [3,5]. Dette kom også fram under forundersøkelsen ved mangel på oppdaterte medisinlister. Et sentralt spørsmål er om e-mail kan gi forbedringer etter at rutinene for bruk er blitt innarbeidet?

3. Bruk av e-mail vil kanskje ikke føre til redusert tidsforbruk. Under forprosjektet nevnte personer fra hjemmetjenesten og legetjenesten at de av og til må vente på telefon og at dette føles stressende. Dette er også bekreftet i litteraturen [3]. Kanskje kan dette unngås ved bruk av e-post.

Målsetting med studien

Undersøke og kartlegge hvorvidt formidling av pasientrelatert informasjon vha PKI-sikret e-mail kan gi en bedre koordinasjon og kommunikasjon mellom hjemmetjeneste og fastlege.

NST ønsker å utrede om e-mail forenkler samarbeidet mellom Stakkevollan og Guleng omsorgstjeneste og Nordbyen og Stakkevollan legesentre. Ifølge Sosial- og helsedepartementet [11] finnes slike ordninger allerede mellom legevakt og primærlege i Danmark:

"..St meld nr 23 (199697) la vekt på betydningen av at legevaktlegen kommuniserer med pasientens fastlege for å sikre kontinuitet i behandlingen. Departementet har vurdert hvordan en slik tilbakemelding skal foretas. I Danmark skjer en slik tilbakemelding automatisk via elektronisk post, uten at legevaktlege har innhentet pasientens samtykke..."

Behandlingsplan
NST vil sammen med IT- ansvarlige i kommunen sørge for en forsvarlig teknisk løsning. Oppkoplingen vil skje etter godkjenning fra Datatilsynet. Nettverket som

koples opp i e-mailforbindelsen, skal også gi legesenter og hjemmetjeneste tilknytning til det nord-norske helsenettet (NH).

Prosjektet skal i størst mulig grad også tilrettelegge for andre nettoppkoplinger som kan være nyttige. F.eks. skal det gis muligheter for kommunikasjon med andre på e-mail som ikke er PKI sikret. Informasjon som går i disse forbindelsene kan ikke være sensitiv. Det samme kan gjelde for legekontorene hvis de f.eks. ønsker tilgang til e-mail lista Eyr[12].

Styret for Programmet for Nord-Norge (PNN) har som hovedmål å bygge opp et statlig finansiert spesialpedagogisk kompetansenettverk i Nord-Norge. Dette nettverket skal være både et alternativ og et supplement til det statlige kompetansesentersystemet i Sør-Norge. PNN driver herunder en virtuell møteplass som heter KomSa [13]. Som en del av KomSa, finnes det også et internt opplysnings- og diskusjonsnett for hjemmetjenester. NST vil undersøke muligheten for at Guleng og Stakkevollan hjemmetjeneste kan tilknyttes dette nettet.

Sikret e-mail forbindelse

NST vil benytte en såkalt public key infrastructure (PKI) løsningen (tilknytning til e-mail vha smartkort og kryptert overføring). Løsningen vil være godkjent av Datatilsynet, og er bl.a. i bruk i Forvaltningsnettet [14].

Datatilsynet aksepterer ikke kun en teknisk løsning, men et sikkerhetskonsept som hver institusjon selv må bygge opp og stå ansvarlig for. NST vil i forbindelse med prosjektet hjelpe Stakkevollan og Guleng hjemmetjeneste og Nordbyen og Stakkevollan legesentere med å skrive søknaden og å utarbeide retningslinjer.

Organisering

Deltagerene i prosjektet bestemmer selv hvilke begrensninger som skal innføres på bruken av e-mail i arbeidet sitt.

Det var i forkant sendt ut et forslag basert på andre studier [15, 16], mens det ble bestemt på innledende prosjektmøte at ingen begrensinger skal gjøres før brukerne har fått prøvd ut forbindelsen i praksis. Det er planlagt et fellesmøte et par uker etter prosjektoppstart.

Det må også avklares hvilken e-mail adresse som skal benyttes. Prosjektet har fått avklart med Datatilsynet at det er mulig å bruke fellesadresser inn til legesentrene fungerende som elektroniske postmottak.

Inklusjonskriterier

Elektronisk post vedrørende alle pasienter med leger fra Stakkevollan eller Nordbyen legesenter som også mottar hjelp fra hjemmetjenesten på Stakkevollan eller Guleng, kan inkluderes. Det kan også inkluderes generelle elektroniske meldinger som ikke er direkte knyttet til en bestemt pasient.

Eksklusjonskriterier

I utgangspunktet er ingen bestemte pasientgrupper utelatt, men det vil bli foretatt en løpende vurderinger av deltagerne med hensyn til innføring av begrensninger i form av regler eller utelatelse av enkelte pasientgrupper. Det vil bli holdt et fellesmøte et par uker etter at prosjektet er igangsatt for å avklare om begrensninger bør gjøres. Deltagerne ifra legesenter og hjemmetjeneste kan også melde ifra ved å bruke e-mail, telefon, faks eller vanlig post til prosjektleder.

Starttidspunkt og gjennomføring

Starttidspunkt vil være umiddelbart etter godkjenning fra Datatilsynet, Statens helsetilsyn og Norsk samfunnsvitenskapelig datatjeneste. Ønsket oppstart er 1. mars. Gjennomføringen vil vare i minst 6 måneder; prosjektperioden vil bli forlenget hvis det ikke er generert nok e-mail for prosjektet. Med "nok e-mail" menes tilstrekkelig mengde til å oppnå statistisk holdbare resultater; her satt til minst 100 e-mail.

Kostnader

Kostnadsbeskrivelse	*Pris (i NOK)*
3 rutere (Cisco 1603)	60 000
2 anti-virus lisenser for små helseinstitusjoner (Norman)	1 000
30 PKI-løsninger	25 000
Installasjonskostnad ISDN og brukerløsning	4 000
Tilsammen	**90 000**

Alle priser er i NOK. Prosjektet har kun intern finansiering. Det gis ikke lønn til prosjektdeltakere utover tilførsel av nytt utstyr.

Internt forbruk av timer for NST er skissert til å være 9 månedsverk fordelt på to personer.

Etiske betraktninger

Etter samtale med Regional komité for medisinsk forskningsetikk helseregion Nord-Norge [17], så denne det ikke som aktuelt å behandle søknaden fordi prosjektet ikke omfattet biomedisin (muntlig tilsagn). Det søkes imidlertid til Datatilsynet [18], Norsk samfunnsvitenskapelig datatjeneste [19] og Statens helsetilsyn [20]. Helsepersonell på legesenter og hjemmetjeneste anonymiserer pasientinformasjon før e-posten blir evaluert.

Resultat, analyse og publikasjon

All mail som sendes ved hjelp av PKI, skal samles opp til prosjektet er avsluttet. I tillegg vil den elektroniske posten ikke bli slettet før en artikkel er godkjent og publisert. Det er beregnet 12 måneder til behandling av data etter prosjektavslutning samt artikkelskriving. Alle data blir liggede på server hos de respektive helseinstitusjonene, slik at ingen sensitiv informasjon skal forsvinne ut fra institusjonens lokaler. Hvis det

skulle bli nødvendig å ta utskrift av eller videresende mail, skal denne være anonymisert først.

I tillegg til å kategorisere e-mailen som blir laget i prosjektet, vil det bli gjennomført en kvalitativ intervju undersøkelse av en med hovedoppgave innen samfunnsfag, eventuelt av en samfunnsfagsstudent på slutten av studiene. Det er ham eller henne som også vil være ansvarlig for gjennomføring av denne delsen av undersøkelsen.

Analyse

Som innledning til prosjektet må det skaffes opplysninger om

- ansatte pr yrkesgruppe på legekontor og hjemmetjenester.
- antall brukere ved Stakkevollan og Guleng hjemmetjeneste totalt.
- hvor mange pasienter som sokner til Stakkevollan og Nordbyen legetjeneste, og fordelingen på den enkelte fastlege.

Selve kartleggingen/evalueringen vil bli en kvalitativ undersøkelse. Kvalitativ undersøkelser er valgt fordi det er gjort lite undersøkelser på dette området tidligere, og man ikke vet hva helsepersonellet opplever som nyttig og negativt. Hjemmetjenesten vil også ha vansker med å fylle ut skjema hver gang de tar kontakt med legesenterene. Dette skyldes både mange ansatte og at hjemmetjenesten ofte kontakter legesenter fra mobiltelefonene mens de er på hjemmevisitt.

Etter prøveperioden gjennomgåes all relevant e-mail og kategoriseres for å forsøke å finne fram til hva e-mail ble brukt til og om e-mail forbindelsen har vært nyttig mhp organisering av rutiner for kommunikasjon og kontakt. Denne kategoriseringen foregår på hver enkelt institusjon der mailen er lagret.

Publikasjoner

-Prosjektet er planlagt presentert på en internasjonal telemedisinkonferanse og/eller Norsk Telemed v/ Siri Uldal.

-Det er planlagt en artikkel til et internasjonalt eller nasjonalt fagtidsskrift. Den ansvarlige er Siri Uldal og evaluator, sannsynligvis Hege Andreassen.

Kopi av artikler og eventuell rapport går til deltagere som ønsker dette, til helsesjef, soneleder og PRO-sjef. Hvis det kan sies at noen av prosjektdeltagerne har deltatt i betydelig grad til prosjektet inkludert artikkelskriving, skal disse inkluderes i forfatterlisten. Takksigelser gis til støttespillere/deltakere som ikke oppfyller krav til forfatterskap.

Referanser

1. Forte PS. The high cost of conflict. Nurse Econ 1997; 15 (3):119-123.
2. Caswell D, Cryer HG. Case study: When nurse and physician don't agree. J Cardiovasc Nurs 1995; 9: 30-42.
3. Cadogan MP, Franzi C, Osterweil D, Hill T. Barriers to Effective Communication in Skilled Nursing Facilities: Differences in Perception between Nurses and Physicians. JAGS 1999; 47:71-75.
4. Statens Helsetilsyn. Rundskriv om kvalitet i pleie- og omsorgstjenesten. I-13/97 www.helsetilsynet.no/regelver/rundskri/1997/i-1397.htm

5. Meighan S, Curran C. Nurse-physician relationship: Getting things rolling. Crit Care Nurse 1992; 12:112.
6. Nylenna M, Hjortdal P, Aasland OG. Internett-bruk blant norske leger. Tidsskr Nor Lægeforen 1999; 119(29): 4342-4.
7. Green L. A better way to keep in touch with patients. Med Econ 1996, 73(20):153-6.
8. Engstrom P. Can you afford not to travel the Internet? Med Econ 1996; 73(13):173-80.
9. Øverbø T. Primærlege går nye veier: -Pasientdagbok gir bedre forestående. Psykisk helse 1999; 4:14-15.
10. Øverbø T. Pilotprosjekt i Norge. Psykisk helse 1999; 4:14-15.
11. Sosial- og helsedepartementet (SHD): Fastlegeordningen. Høringsnotat. Midlertidig versjon 201098. http://www.odin.dep.no/shd/norsk/publ/hoeringsnotater/030005-990336/index-hov009-b-n-a.html#kap9 http://odin.dep.no/shd/publ/1998/fastlegehoering/del9.html#P3557_305721
12. Eyr –epostliste for allmenpraktikere. http://www.uib.no/isf/eyr/eyr.htm
13. KomSa – kommunikasjon og samhandling i nettverk. http://www.komsa.no
14. Forvaltningsnettet. http://www.forvaltningsnett.dep.no
15. Guidelines for the Clinical Use of Electronic Mail with Patients, JAMIA, 1998; 5:104-111.
16. Stanford Medical Group. Electronic Mail Services. http://www-med.stanford.edu/shs/smg/email
17. Den nasjonale forskningsetiske komite for medisin. http://www.etikkom.no/NEM/nem.htm
18. Datatilsynet. http://www.datatilsynet.no
19. Norsk Samfunnsvitenskapelig datatjeneste (NSD). http://www.nsd.uib.no/personvern/
20. Statens helsetilsyn. http://www.helsetilsynet.no/

Sikkerhetshåndbok

For små helseinstitusjoner

Innhold

Avviksbehanding

Avviksrapport, <institusjon>			
Formål: Rapporten skal sikre at alle brudd og antatte brudd på sikkerhetsrutinene blir registrert og behandlet på forsvarlig måte.			
Beskrivelse av avviket/mulig grunn for avvik:			
Melderens navn:		*Dato/klokkeslett:*	
Beskrivelse av iverksatte tiltak:			
Kontakt med NH:			
Sikkerhetsan-svarliges /nestansvarliges behandling	*Klassifikasjon*/skal være utbedret innen dato:*	*Datatilsynet varsles JA/NEI*	*Dato/underskrift:*

**1.Svært alvorlig/ må ordnes innen 24 timer.*
2. Middels alvorlig/utbedres snarest.
3. Ikke alvorlig/ utbedres ved anledning

Ansvar

Ansvarlig, data og sikkerhet og nestansvarlig vil rapportere til ledelsen og ha ansvar for at informasjon om data og sikkerhet blir formidlet til alle ansatte.

Ansvarlig, data og sikkerhet: <navn>
Nestansvarlig, data og sikkerhet: <navn>[1]

Sikkerhetsmål

Å behandle personopplysninger i samsvar med helsepersonelloven – herunder journalforskriften, og personopplysningsloven – herunder sikkerhetsbestemmelsene i personopplysningsforskriften.
<helseinstitusjonen> skal ha et akseptabelt sikkerhetssystem som gjør det mulig for brukerne av informasjonssystemene å samhandle sikkert, korrekt og med nødvendig tilgjengelighet internt og eksternt. Dataanlegget skal også kunne brukes til opplæring, informasjonstilgang og privat bruk så sant det ikke strider imot formål om å behandle personopplysninger sikkert. Hjemmekontor er foreløpig ikke tillatt.

Sikkerhetsstrategi

Retningslinjer
En sikkerhetshåndbok utarbeides, som skal inneholde dokumenterte retningslinjer for bruk av
Internett, e-post og tilgang til registre. Disse retningslinjene skal være kjent for alle ansatte.

Fysisk sikring
Alle maskiner der det blir lagret sensitive personopplysninger, skal plasseres på avlåste steder.

Teknologi
Virksomheten skal benytte teknologi og løsninger som gjør det mulig å hindre utlevering av sensitiv informasjon av vanvare. Det skal etableres teknologiske løsninger som hindrer at uvedkommende får tilgang til virksomhetens systemer via eksterne nett.

Risikoanalyse
I sikkerhetshåndboken er det innebygd en risikoanalyse med risikoreduserende tiltak som alltid skal benyttes. Ved større omlegginger skal det vurderes om spesielle risikovurderinger må gjøres.

Prosedyrer
Sikkerhetshåndboken skal inneholde dokumenterte prosedyrer som alltid skal følges.

Forhold til leverandører
Legesenteret har satt bort lokal drift til <IT driftsfirma> og for nettverk og ruter til NH. Daglige operasjoner vedrørende drift og backup tar legesenteret seg av selv. Forhold til alle leverandører skal kontraktsfestes, også mhp sikkerhet og taushetserklæring underskrives der det er aktuelt.

[1] I denne beskrivelsen legges det opp til at ansvarlig for data og sikkerhet er den legen som har dataansvar på legesenteret, og nestansvarlig er den helsesekretæren som tar backup og ordner med nøkler til nyansatte.

Sikkerhetsrevisjon
Sikkerhetsrevisjon skal gjøres årlig, imellom 1. sept og 1. okt. og når større oppgraderinger i nettverket er utført.

<underskrift, rep fra ledelsen>
Rep for virksomhetens ledelse

Personopplysninger

Opplysning/ formål	Underpunkt	Hjemmel	Klassifisering	Omfang	Lagring/ kommunikasjon	Kritisk mhp konfidensialitet, integritet eller tilgjengelighet
Lønn og personal: -lønns-opplysn -personal-opplysn		Forskrifter om lov om personreg §2-12	Personoppl. på papir-form.	<hvor mange pers, hva slags opplysninger>	<hvor og hvordan opplysningen er lagret og om de videresendes>	
Helse opplysn: Pasient-journal (ProfDoc)		Helse-personelloven	Sensitive person-opplysn.			Kritisk mhp konfidens-ialitet/integritet/tilgjengelighet
Helse opplysn: Pasient-journal (ProfDoc)	Eks: Spirometri (Spirare)	Helse-personelloven	Sensitive person-opplysn.			Kritisk mhp konfidensialitet/ integritet/ tilgjengelighet
Helse opplysn: Pasient-journal (ProfDoc)	Eks: Labsvar fra RiTø klin. kjem. /immunlogi/ mikrobiol.	Helse-personelloven	Sensitive person-opplysn.			Kritisk mhp konfi-densialitet/integritet/ tilgjengelighet
Helse opplysn: Pasient-journal (ProfDoc)	Eks: E-mail til hjemme-tjenesten	Helse-personelloven	Sensitive person-opplysn.			Kritisk mhp konfidensialitet/integritet/ tilgjengelighet
Hendelses-register: -logg over brudd		Forskr om lov om person-reg §2-12	Sensitive sikkerhets-opplysn. Info om sikkerhets-tiltak			Kritisk mhp konfidensialitet

RISIKOVURDERING

Virksomhet: <helseinstitusjon>								**Dato/sign.:**
RISIKO FØR KONTROLLTILTAK			**KONTROLLTILTAK og LEDEROPPFØLGING**			**RESTRISIKO**		
Hva kan gå galt?	**Kritisk mhp konfiden-sialitet, integritet eller tilgjengelighet**	**Gradering av konse-kvens**	**Hvilke kontrollhandlinger skal iverksettes/ er iverksatt**	**Dokumentasjon av kontrollen**	**Gradering av sann-synlighet**	**Akseptabel restrisiko? (ja/nei)**	**Oppfølging (hvis ikke akseptabel restrisiko)**	**Referanse egenkontroll-skjema**
Fysisk skade på sensitive opplysninger gjennom brann, overoppheting, vannskade etc.	Tilgjengelighet/ integritet	1 – stor	<beskriv kontrollhandinger og tiltak>	Brannansvarlig sørger for at sikkerhetsforskriftene er overholdt ved sjekk minst en gang årlig. Ved mangler skal dette noteres i sikkerhetshåndboken og utbedres snarest.	3-liten	Ja		3.1 / 6.3
Ulovlig inntrenging ved fysisk innbrudd (herunder vandalisme)	Tilgjengelighet/ integretet/ konfidensialitet	3 - stor		Forsøk på inntrenging skal registreres som avvik i sikkerhetsprotokoll og følges opp.	3 -liten	Ja		3.1
Forsøk på ulovlig tilgang til sensitiv opplysninger gjennom inntrenging gjennom datanettet (”hacking”)	Konfidensialitet/ Integritet/tilgjengelighet	1 - stor		Alle avvik registreres i sikkerhetsprotokoll og følges opp. Alle logger følges opp kontinuerlig.	1-stor	Ja		4.1/ 5.1/ 6.2/ 6.3

Virksomhet: <helseinstitusjon>								Dato/sign.:
RISIKO FØR KONTROLLTILTAK			**KONTROLLTILTAK og LEDEROPPFØLGING**			**RESTRISIKO**		
Hva kan gå galt?	**Kritisk mhp konfiden-sialitet, integritet eller tilgjengelighet**	**Gradering av konse-kvens**	**Hvilke kontrollhandlinger skal iverksettes/er iverksatt**	**Dokumentasjon av kontrollen**	**Gradering av sann-synlighet**	**Akseptabel restrisiko? (ja/nei)**	**Oppfølging (hvis ikke akseptabel restrisiko)**	**Referanse egenkontroll-skjema**
Helsesekretærer eller legekolleger på senteret får tilgang til pasientopplysninger de ikke har behov for å kjenne til	Konfidensialitet	3- liten	Eks: Alle ansatte på legesenteret er underlagt taushetsplikt enten gjennom sin utdannelse (helsesekretærer, jordmor og leger) eller ved underskrift (renholdsbetjent), slik at pasienter som kommer på legesenteret skal være beskyttet. I tillegg er pasientjournal og det lokale nettverket passordtilknyttet. Passordbeskyttede skjermsparere slår seg på hvis PC ikke har vært brukt de siste 10 minutter. Det er meget liten turn-over på legesenteret og få ansatte så alle kjenner hverandre.	Årlig sjekk. Avvik reg. på avviksskjema	3-liten	ja		2.1 /3.1
Noen av legekontorets ansatte bryter taushetsplikten. Sensitive opplysninger kommer på avveie.	Konfidensialitet	1-stor	Eks: Ved mistanke om brudd på taushetsplikten har medansatte plikt på seg til å melde ifra til legesenterets ledelse. Ledelsen vil vurdere forholdene og gå til anmeldelse hvis de finner at taushetsplikten er blitt brutt.	Behandles forløpende. Reg. på avviksskjema	3-liten	ja		2.1
Virusprogram eller annen ødeleggende programvare kan skade opplysninger som er viktige for virksomheten (fortrinnsvis pasientopplysninger). Herunder også trussel om at legesenteret kan spre ødeleggende programvare videre til andre helseinstitusjoner i vanvare eller med overlegg.	Integritet/ tilgjengelighet	1-stor	Eks: Siste versjon av virusprogram skal være installert på alle PC'er og server (tilgang til siste versjon via kontrakt med NH). I tillegg får alle ansatte informasjon om å være kritiske til å ta i bruk disketter som de på forhånd ikke vet hvor kommer ifra eller ikke er sikker på innholdet i. Det skal heller ikke installeres programmer som ikke på forhånd er blitt godkjent av sikkerhetsansvarlig på legesenteret. Mail med vedlegg skal ikke åpnes med mindre man kjenner avsender og/eller vet hva innholdet i sendingen er.	Behandles fortløpende. Reg. på avviksskjema.	1-stor sannsynlighet	ja		0.1/0.2 /0.3 / 0.4 /0.5/ 3.1 /4.1

Virksomhet: <helseinstitusjon>								Dato/sign.:
RISIKO FØR KONTROLLTILTAK			**KONTROLLTILTAK og LEDEROPPFØLGING**			**RESTRISIKO**		
Hva kan gå galt?	**Kritisk mhp konfiden-sialitet, integritet eller tilgjengelighet**	**Gradering av konse-kvens**	**Hvilke kontrollhandlinger skal iverksettes/er iverksatt**	**Dokumentasjon av kontrollen**	**Gradering av sann-synlighet**	**Akseptabel restrisiko? (ja/nei)**	**Oppfølging (hvis ikke akseptabel restrisiko)**	**Referanse egenkontroll-skjema**
Bevisst eller ubevisst sabotering/ødelegging av data fra ansatte på legesenteret.	Integritet/tilgjengelighet	1 - stor	Eks: <helsinst> har liten turn-over og få ansatte. Backup rutiner vil til også beskytte for ødeleggelse fra egne ansatte. I tillegg finnes passord rutiner. Ubevisst sabotasje forsøkes unngått ved å holde medarbeidere innformert og oppdatert så langt mulig.	Behandles fortløpende. Reg på avviksskjema	3 - liten	ja		6.3
Ansatte hos partnere misbruker taushetsplikten eller kontraktsavtalen slik at sensitive opplysninger blir tilgjengelige for uvedkommende.	Konfidensialitet	1 - stor	Eks: Forholdet til alle partnere som ikke er norske helseinstitusjoner er kontraktsbundet slik at taushetsplikt avkreves og informasjons gis. Andre norske helseinstitusjoner vil automatisk være underlagt taushetsplikt om pasientinformasjon. Legesenteret har oversikt over hvem som har fått tilgang til forskjellige opplysninger på legesenteret gjennom oppgitte kontaktpersoner.	Underskrift på taushetserklæring fra ansatte hos partnere. Kontrakter med partnere.	3-liten	ja		6.1 / 8.1
Pasienter/besøkende får tilgang på sensitiv informasjon eller ødelegger data/datatilgang inne på legesenteret.	Konfidensialitet/ tilgjengelighet/ integritet	1- stor	Eks: Det er satt på skjermbeskyttere som slår seg inn etter 10 min. PC skjermene er ikke vendt mot pasientene.	Årlig egenkontrol. Avvik registreres i avviksprotokoll.I				3.1/ 3.2 / 3.3 / 6.4
Helsepersonell sender i vanvare ut sensitiv informasjon til uvedkommende	Konfidensialitet	1 - stor			3-liten			4.1

Egenkontroll av Informasjonssikkerhet

Virksomhet: Tidsrom:

Nr	OMRÅDE/KONTROLLHANDLING Referanse til underliggende dokumentasjon	Virksomhetens vurdering JA NEI	Ansvarlig for Utføring / Tidspunkt	Dokumentasjon	Dato / Sign. av Ansvarlig
Overordnet om informasjonssikkerhet					
0.0	**Blir resultatene fra sist gjennomførte egenkontroll tatt med som del av kriteriene for gjennomføring av denne kontrollen?**	☐ ☐			
0.1	**Er virksomhetenes policy for informasjonssikkerhet godt kjent av alle tilsatte ?**	☐ ☐			
0.2	**Er sikkerhetshåndboken oppdatert med eventuelle endringer?**	☐ ☐			
0.3	**Er alle tilsatte kjent med at virksomheten har en håndbok i informasjonssikkerhet?**	☐ ☐			
0.4	**Har virksomheten fordelt roller og ansvar til sikkerhetsansvarlig og nestansvarlig?**	☐ ☐			
0.5	**Har personell som er tildelt rolle(r) for sikkerhet tilstrekkelig tid og**				

	kompetanse til å utføre sine oppgaver?				
	<u>Avsluttende vurdering etter at kontrollskjemaet er ferdig utfylt:</u> **Finnes det andre områder innen informasjonssikkerhet, som ikke er tatt med i kontrollskjemaet, og som medfører uakseptabel risiko for virksomheten?**	☐ ☐			

Egenkontroll av Informasjonssikkerhet

Virksomhet: Tidsrom:

Nr	OMRÅDE/KONTROLLHANDLING Referanse til underliggende dokumentasjon	Virksomhetens vurdering JA	 NEI	Ansvarlig for Utføring / Tidspunkt	Dokumentasjon	Dato / Sign. av Ansvarlig
1	**Løpende kontrollaktiviteter**					
1.2	**RISIKOVURDERINGER** **Gjennomføres løpende risikovurderinger som beskrevet i håndbok i informasjonssikkerhet?**	☐	☐			
1.3	**EGENKONTROLL** **Gjennomføres egenkontrollen (dette skjema) minst en gang årlig?** **Blir risikoer dokumentert (risikoskjema) , vurdert og eventuelle tiltak iverksatt?**	☐ ☐	☐ ☐			
1.4	**LØPENDE AVVIKSBEHANDLING** **Har virksomheten etablert prosedyre for registrering og oppfølging av avvik ?**	☐	☐			

Egenkontroll av Informasjonssikkerhet

Virksomhet: Tidsrom:

Nr	OMRÅDE/KONTROLLHANDLING Referanse til underliggende dokumentasjon	Virksomhetens vurdering JA NEI	Ansvarlig for Utføring/ Tidspunkt	Dokumentasjon	Dato / Sign. av Ansvarlig
2	**Personell sikkerhet**				
2.1	**TAUSHETSERKLÆRING** **Har alle med tilgang til virksomhetens informasjon (IT-systemer, lokaler, arkiv m.m) undertegnet siste utgave av taushetserklæring?**	☐ ☐			
2.2	**ENDRING OG OPPHØR AV STILLING/FUNKSJON** **Har virksomheten tilfredsstillende prosedyrer som ivaretar endringer eller slutt av arbeidsforholdet (inndragelse nøkler, passord, smartkort o.l.)?**	☐ ☐			
2.3	**OPPLÆRING OG BEVISTGJØRING** **For personell nødvendig opplæring og veiledning i informasjonssikkerhet ?** **Har de ansatte fått opplæring i hvordan de kan hindre inntrenging og spredning av datavirus?**	☐ ☐ ☐ ☐			

Egenkontroll av Informasjonssikkerhet

Virksomhet: Tidsrom:

Nr	OMRÅDE/KONTROLLHANDLING Referanse til underliggende dokumentasjon	Virksomhetens vurdering JA	Virksomhetens vurdering NEI	Ansvarlig for Utføring / Tidspunkt	Dokumentasjon	Dato / Sign. av Ansvarlig
3	**Fysisk sikkerhet**					
3.1	**SIKREDE OMRÅDER** **Har virksomheten innført tiltak om fysisk sikring vurdert ut fra risiko ?** **Er skrivere plassert slik at de ikke medfører sikkerhetsrisiko?** **Er det utført tilstrekkelige tiltak mot brann- og vannskader?** **Er det uført tilstrekkelige tiltak mot innbrudd?** **Er ansatte flinke nok til å låse dørene både i og etter arbeidstid?**	☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ 			
3.2	**ARBEIDSPLASSEN** **Er arbeidsplassen utformet slik at den ikke medfører risiko for innsyn (f.eks. er alle PC'er utstyrt med passord på skjermsparer)?**	☐	☐			

	Holdes arbeidsplassene ryddige, slik at personopplysninger ikke kommer på avveier?	☐ ☐			
3.3	**FYSISK SIKKERHET FOR ØVRIG** **Finnes det for øvrig mangler som medfører uakseptabel risiko?**	☐ ☐			

4 Elektronisk samhandling

4.1	**INTERNETT** **Har virksomheten kontroll med bruken av Internett?** **Har virksomheten kontroll med bruken av e-post?** **Er det sikkert at ikke sensitive opplysninger blir sendt ut til uvedkommende?**	☐ ☐ ☐ ☐ ☐ ☐			

Egenkontroll av Informasjonssikkerhet

Virksomhet: Tidsrom:

Nr	OMRÅDE/KONTROLLHANDLING Referanse til underliggende dokumentasjon	Virksomhetens vurdering JA NEI	Ansvarlig for Utføring / Tidspunkt	Dokumentasjon	Dato / Sign. av Ansvarlig
5 Teknisk sikkerhetsløsning					
5.1	**TEKNISK LØSNING** **Er de tekniske løsningene iht. personopplysningsforskriften ?**	☐ ☐			
6 **Sikring av informasjon**					
6.1	**AUTORISASJON OG TILGANGSKONTROLL** **Er all tilgang til informasjon gitt i henhold til tjenstlige behov?** **Revurderes tilganger ved behov og minst en gang årlig?** **Hvis aktuelt, er eksterne partnere og leverandører regulert med kontrakt og taushetsreklæringer?**	☐ ☐ ☐ ☐ ☐ ☐			

6.2	**DATAVIRUS OG DATAINNTRENGING** **Er siste versjon av antivirusbeskyttelse lastet ned fra NHs hjemmesider?** **Gjennomgåes alle logger regelmessig?**	☐ ☐ ☐ ☐			
6.3	**SIKKERHETSKOPIERING** **Virker prosedyrene for sikkerhetskopiering hensiktsmessige (f.eks. finnes det en oppdatert sikkerhetskopi av journal utenfor legesenteret)?** **Testes langtidstape minst en gang hvert år?** **Ligger sensitiv informasjon kun på server eller finnes kopier på lokale disker?**	☐ ☐ ☐ ☐ ☐ ☐			

Egenkontroll av Informasjonssikkerhet

Virksomhet: Tidsrom:

Nr	OMRÅDE/KONTROLLHANDLING Referanse til underliggende dokumentasjon	Virksomhetens vurdering JA NEI	Ansvarlig for Utføring / Tidspunkt	Dokumentasjon	Dato / Sign. av Ansvarlig
6.4	**SLETTING** **Har virksomheten prosedyrer for sletting av data medier og papir ?** **Blir all informasjon slettet fra harddisker og lagringsmedia før disse kasseres?**	☐ ☐ ☐ ☐			

7 Dokumentasjon

7.1	**Er sikkerhetspermen tilgjengelig og oppdatert** **Er alle avvik i behandlingsskjema tatt tilfredsstillende hånd om?**	☐ ☐ ☐ ☐			

8 Informasjon om partnere og leverandører

8.1	**Underskriver partnere og leverandør taushetserklæring ?** **Er alle kontrakter med partnere på plass og tilgjengelige?**	☐ ☐ ☐ ☐			

Organisering

Organisasjonskart:

<Organisasjonskart>

Legesenteret har i dag følgende ansatte:
Leger: <tall>
Legesekretærer: <tall>
Jordmor: <tall>
Renholdsbetjent: <tall>
Andre: <turnuskandidater etc.>

Kort beskrivelse av virksomheten:
Virksomheten er privatdrevet, men med fastlegetilskudd etter avtaler med kommunen.
Legesenteret er regulert av avtaler med kommunen gjennom fastlegetilskuddet.
<Ledelsesstruktur; fordeling av overskudd og utgifter>

Oppgaver, ansvarlig datasikkerhet

1) Ved avvik: varsle ledelsen, ansatte, NH og andre partnere hvis aktuelt. Varsle Datatilsynet og politiet om avviket hvis det er av svært alvorlig karakter.

2) Ved avvik: Sørge for protokollføring og nødvendige tiltak for å stoppe avviket samt være ansvarlig for at avviket opphører.

3) Sørge for en årlig gjennomgang av datasikkerheten på legesenteret sammen med ledelse, nestansvarlig og om nødvendig partnere imellom 1. sept og 1.okt. Gjennomgå datasikkerhetsrutinene også ved store oppgraderinger, endringer eller utvidelser av informasjonssystemene.

4) Sørge for at datainnkjøp, -endringer eller -utvidelser er i henhold til sikkerhetspolicy.

5) Ansatte med datakompetanse må alltid være tilgjengelig selv ved sykdom og ferier.

6) Ha ansvar for kontroll av lokale datalogger.

7) Ha oversikt over hvem som har tilgang til sensitive opplysninger og deres datarettigheter for innsyn og skriving.

8) Sørge for installasjon av siste versjon av viruskontroll på alle maskiner.

9) Sørge for at ledelsen har innført gode rutiner for forholdsregler ved brann, vannlekkasje og fysisk innbrudd enten det utføres av sikkerhetsansvarlig selv eller andre på legesenteret.

10) Sørge for at alle rom med datautstyr holdes fysisk avlåst når rommene ikke er i bruk.

11) Sørge for at det finnes kontrakt med partnere om datasikkerhet.

12) Holde seg selv og nestansvarlig oppdatert på forandringer som partnere innfører.

13) Sørge for at alle ansatte er oppdatert på gjeldende sikkerhetsforskrifter og kjenner til bakgrunnen for reglene (se informasjon til alle ansatte). De ansatte må også vite hvem som er datasikkerhetsansvarlig og –nestansvarlig.

14) Sørge for god nok dokumentasjonskontroll for legesenteret.

Oppgaver, nestansvarlig datasikkerhet

1) Har ansvar for datasikkerhet når ansvarlig for datasikkerhet er borte.

2) Rapporterer til ansvarlig for datasikkerhet ved avvik.

3) *Delegert ansvar:* Sørge for at tilstrekkelig autorisasjon og nøkler blir gitt nyansatte og at dette trekkes tilbake senest to måneder etter avsluttet arbeidsforhold.

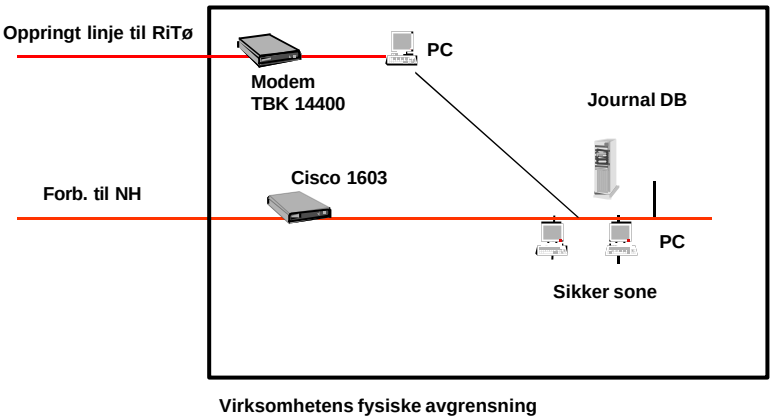
4) *Delegert ansvar:* Sørge for at alle ansatte og aktuelle partnere har skrevet under på taushetserklæring ved arbeidsstart eller godtatt taushetsplikt gjennom sin utdanning.

5) *Delegert ansvar:* Sørge for at helsesekretærer er oppdatert på gjeldende sikkerhetsforskrifter og kjenner til bakgrunnen for reglene (se informasjon til alle ansatte).

Konfigurasjon

Konfigurasjonskart

<eksempel:>



Fysisk sikkerhet

<Dokumentasjonsrutiner ikke avklart>

Systemteknisk sikkerhet

<Dokumentasjonsrutiner ikke avklart>

Partnere og leverandører

Partnerens navn	**Funksjon/oppgave**	**Ansvar fysisk / systemteknisk sikkerhet, tilknytning**	**Kontrakt**	**Kontaktperson**
<Lokalt IT-firma>	Drift og vedlikehold av dataanlegg på legesenteret	Fysisk/systemteknisk	Se vedlegg	<navn, tlf>
Nord-Norsk Helsenett (NH)	Drift og vedlikehold av sikkerhetsløsning og intern sone	Fysisk/systemteknisk Tilknyttet elektronisk	Se vedlegg	77754900 sentralbord
<Journalleverandør>	Ansvar for pasientjournal	Systemteknisk	<lokalt IT-firma> eller sikkerhetsansvarlige vil utføre endringer og oppgraderinger på legesenteret. <Journallev > vil derfor kun være å regne som en sw leverandør.	< servicesenter, tlf>.
<Vekterselskap>	Patruljerer bygningen	Fysisk		

Informasjonssikkerhet

Det er deg det kommer an på!

LOGG DEG INN!
Bruk alltid ditt eget brukernavn og passord – aldri andres. Passordet er hemmelig.
Snapper andre opp passordet ditt, skal du skifte det umiddelbart og rapportere det til nærmeste overordnede.
Skriv ikke passordet på lapper gjemt på lure steder.

HJELP EN KOLLEGA
Minn hverandre om informasjonssikkerheten.

HVIS DU OPPDAGER ET AVVIK
Sørg for å melde ifra til datasikkerhetsansvarlig eller -nestansvarlig, og protokollfør avviket.

BRUK BARE GODKJENT UTSTYR!
Av sikkerhetsmessige grunner er det ikke tillatt å koble egne maskiner til nettverket. Modem er ikke tillatt.
Private disketter og CD-er skal på forhånd sjekkes nøye for virus.

VERN DEG MOT INNSYN
Gå ikke fra skjermen når programmer og data er tilgjengelige. Beskytt datskjermen din mot innsyn fra vinduer og korridorer.

TING SOM FLYTER
Utskrifter som flyter, kan røpe mangt og mye. Hent utskriftene dine, pass på at andre ikke får innsyn i informasjonen de inneholder. Disketter og CD-er skal destrueres.

LOGG DEG UT
Logg deg alltid ut av sensitive systemer når du ikke er på plassen din, enten det er til lunsj, når du har pause, eller når du går for dagen.

Strategi mot virus

Brukere

Det er installert et antivirusprogram som aktiveres hver gang datamaskinene blir slått på. Programmet må alltid være aktivt, slik at en har kontroll uten brukermedvirkning.

Kontroller alltid disketter og CD-er som kommer utenfra, før de leses inn i datamaskinene.

Kontroller alltid elektroniske vedlegg til e-post før de åpnes.

Vær alltid kritisk til vedlegg til e-post når du ikke kjenner avsenderen fra før.

Hent ikke ned programmer via nettverket uten å ha kontaktet datasikkerhetsansvarlig først.

Teknisk

Kontakt eksperthjelp hvis du har mistanke om at PC'en har blitt virusinfisert.

Legg ikke tilbake sikkerhetskopien før det er sikkert at eventuelle datavirus er fjernet.

Sikkerhet ved bruk av Internett

Internettsikkerhet

Alle ansatte skal vite hva som anses som god praksis når en representerer virksomheten på Internett – også kalt nettikette.

All oppkobling til Internett skal skje gjennom virksomhetens sikkerhetsløsning. Det er ikke tillatt å koble seg til Internett på andre måter, for eksempel via et lokalt modem på PC-en.

Det er strengt forbudt å benytte virksomhetens IT-systemer til aktiviteter som bryter med norsk lov.

Alle filer og all programvare som lastes ned, skal godkjennes av datasikkerhetsansvarlig og kontrolleres for virus før de åpnes eller kjøres.

Regler ved bruk av e-post

Reglier for bruk av sikret/sensitiv e-post
Husk at du ikke har noen garanti for at meldingen når mottakeren. **Kontroller adresser – send til korrekt mottaker.** **Vær oppmerksom på adresselister – alt sendes til alle.**

Regler for bruk av usikret e-post
Tenk igjennom hva du skriver – vanlig e-mail kan leses av uvedkommende. **Fare for virus: Programfiler (.exe filer) skal ikke åpnes uten at du vet innhold og kjenner avsender.** **Vær spesielt oppmerksom på adresselister – alt sendes til alle.** **Hvis du vil unngå uadressert reklame, bør du ikke delta i nyhetsgrupper/e-mail lister eller på andre måter offentliggjøre din e-mail adresse på Internett. Gjør du likevel dette, anbefales det å opprette en egen e-mail adresse som lett kan stenges.**

Taushetserklæring

Denne erklæringen er en del av kontrakt mellom

bruker _____og

partner/leverandør _____
inngått

(sted og dato):_____

Undertegnede er ansatt hos partner/leverandør og skal utføre oppdrag der jeg kan få tilgang til program, utstyr eller områder der personsensitiv informasjon behandles. Ved å undertegne denne erklæringen forsikrer jeg at jeg i mitt arbeide vil bevare taushet om personopplysninger og sikringstiltak som jeg får kjennskap til.

Jeg er innforstått med at brudd på taushetsplikten kan føre til kontraktsbrudd og påfølgende erstatningskrav. Brudd på taushetsplikten kan videre medføre tjenestelige reaksjoner. Dersom oppdraget utføres for bruker som er en kommunal eller fylkeskommunal tjenesteyter er jeg underlagt taushetsplikt etter forvaltningsloven § 13 og brudd på denne kan medføre straffeansvar etter straffeloven § 121.

Jeg er innforstått med at taushetsplikten også gjelder etter at oppdraget er utført og etter at jeg har sluttet i tjenesten hos min arbeidsgiver.

Sted og dato:
_____

Fødselsdato: _____

Underskrift