Prosjektrapport

Kommunikasjonsnettverk for privat og offentlig tannhelsetjeneste i Nord-Norge

En teknologisk og organisatorisk utredning av fagnett for ansatte i tannhelsetjenesten i Nord-Norge

Fra NST: Terje Solvoll, Eva Henriksen og Erlend Bønes.
Fra TkNN: Håkon Edvardsen og Jorunn Nyheim

Tittel:	**Kommunikasjonsnettverk for offentlig og privat tannhelsetjeneste i Nord-Norge**
NST-rapport:	06-2007
Prosjektleder:	Terje Solvoll
Forfattere:	Terje Solvoll, Eva Henriksen, Erlend Bønes, Håkon Edvardsen og Jorunn Nyheim
ISBN:	978-82-92092-84-2
Dato:	22.05.2007
Antall sider:	39
Emneord:	Teknologiske utfordringer, organisatoriske utfordringer, fagnett
Oppsummering:	Denne rapporten er en utredning av teknologiske og organisatoriske utfordringer ved etablering av kommunikasjonsplattform og fagnettløsning for tannhelsetjenesten i Nord-Norge. Rapporten støtter seg til konklusjonene i den nasjonale rapporten om "Elektronisk kommunikasjon i tannhelsetjenesten", og viderefører denne med å utføre en del av de foreslåtte utredningene. Rapporten oppsummerer flere nettverksteknologier og fagnettløsninger, og avslutter med en anbefaling om å gjennomføre et pilotprosjekt med ca. 40 spesialiser, med oppstart høsten 2007. Valget av nettverksleverandør har i anbefalingene falt på Norsk Helsenett, og når det gjelder fagnettløsning er anbefalingen Helsekompetanse.no. Anbefalingen av meldingsutveksler (EDI) falt på Well Communicator.
Utgiver:	Nasjonalt senter for telemedisin Universitetssykehuset Nord-Norge Postboks 35 9038 Tromsø Telefon: 77 75 40 00 E-post: info@telemed.no Internett: www.telemed.no

Forord

Tanken bak denne rapporten er å utrede mulighetene for et elektronisk nettverkssamarbeid i Nord-Norge med mulig utvidelse til resten av landet, slik at tannhelsetjenesten kan ta i bruk elektronisk verktøy for å etablere bedre kommunikasjon seg i mellom, formidle bedre informasjon ut til pasienter, og legge grunnlag for elektronisk samhandling med samarbeidspartnere. E-læring, prosedyrebeskrivelse/video og kompetanseheving er også et tema i rapporten.

Rapporten er gjort på oppdrag fra Tannhelsetjenestens kompetansesenter for Nord-Norge (TkNN)

Takk til prosjektdeltakerne, Elin Johnsen, og Kristin Sandvik og Øystein Fredriksen, samt innspill fra tannhelsepersonell i Sør-Troms.

Tromsø 22.05.2007

Terje Solvoll, Eva Henriksen, Erlend Bønes, Håkon Edvardsen og Jorunn Nyheim.

Innhold

1 Hensikten med prosjektet 7
1.1 Bakgrunn 7
1.2 Målet med prosjektet 7

2 Eier, kunde og andre interessenter 8
2.1 Eier 8
2.2 Kunde 8
2.3 Andre interessenter 8

3 Brukere 8
3.1 Brukere av systemet 8
3.2 Brukerprioritet 8
3.3 Brukermedvirkning 8

4 Begrensinger 8

5 Relevante fakta 10
5.1 Navnekonvensjoner og definisjoner 10
5.2 Løsninger 10
5.3 Omgivelser 10
5.4 Applikasjoner som produktet skal samhandle med 10
5.5 Annen kommersiell programvare 11
5.6 Forutsetninger 11

6 Produktbeskrivelse 11
6.1 Fagnettets innhold 11
6.2 Brukergrensesnitt 12

7 Funksjonelle krav 13
7.1 Funksjonelle krav for ny løsning 13

8 Ikke-funksjonelle krav 14
8.1 Utseende 14
8.2 Brukervennlighet 14
8.3 Ytelse og kapasitet 14
8.4 Operasjonelle krav 14
8.5 Vedlikeholdskrav og krav til systemuavhengighet 15
8.6 Sikkerhetskrav 15
8.7 Juridiske krav 15

9 Organisatoriske utfordringer 16
9.1 Bakgrunn for fagnett 16
9.2 Organisatoriske utfordringer 16
9.3 Utbygging av elektronisk infrastruktur 17
9.4 Fokus på implementering 18

10 Presentasjon av sikrede nettverksløsninger 18
10.1 Norsk Helsenett 18

10.2 Norsk Tannhelsenett 19
10.3 Andre løsninger 20

11 Presentasjon av fagnettløsninger 20
11.1 Classfronter 21
11.2 It's learning 22
11.3 Atutor 22
11.4 Helsekompetanse.no 22
11.5 Well Community 23
11.6 Visma Unique 24
11.7 Unident – C-takt LINK 24

12 Drøfting og tilrådninger 24
12.1 Nettverksløsninger 25
12.2 Fagnettløsning og annen programvare 25
12.3 Økonomi- og tidsestimat for pilotprosjekt 26

Referanser 27

Vedlegg 1: Informasjonssikkerhet og risiko 29
1.1. Juridisk rammeverk 29
1.2. Om informasjonssikkerhet 30
1.3. Om risikoanalyse 31
1.4. Trusler, risiko og mulige tiltak 37

1 Hensikten med prosjektet

1.1 Bakgrunn

Tannhelsetjenestens kompetansesenter for Nord–Norge (TkNN) er oppdragsgiver for dette prosjektet. Kompetansesenteret er tannhelsevesenets ”sykehus”. Her behandles henviste pasienter av spesialister, tannleger utdannes til spesialister og det drives forskning, etterutdanning og veiledning. Kompetansesenteret utvikler og anvender telemedisinsk teknologi.

Det ønskes etablert et elektronisk nettverkssamarbeid i regionen, der spesialister og allmennpraktikere kan delta etter behov eller eget ønske. Det er også ønskelig at nettverket skal kunne brukes til videreutdanning, kursing og faglig oppdatering av ansatte i tannhelse-tjenesten i Nord-Norge. Hensikten er å styrke faglig interaksjon mellom ansatte i tannhelse-tjenesten i landsdelen.

På denne måten ønsker man å oppnå følgende:

1. Å få bedre oversikt over hvilken kompetanse man faktisk har i regionen, og mulighetene for å hente inn denne etter behov. Dette gjelder kompetanse på behandling, undervisning, veiledning og kursgjennomføring.
2. Å styrke samarbeid om enkeltkasus og temaer hvor det er ønskelig eller nødvendig.
3. Utveksling av erfaringer og synspunkter – kompetanseheving.
4. Styrke fellesskapsfølelsen – gjøre det mer attraktivt å arbeide utenfor store klinikker/sentra.
5. Muliggjøre elektronisk sending/mottak av henvisning og epikrise.

Tannhelsetjenesten i Nord-Norge sliter med rekrutteringen, og i denne forbindelse ønsket TkNN prosjektleder, sosiologisk og teknologisk kompetanse fra NST (Nasjonalt Senter for Telemedisin) for utredningen av et fagnett.

1.2 Målet med prosjektet

TkNN ønsker en elektronisk kommunikasjonsplattform for tannhelsetjenesten (allmenn-tannleger, spesialisttjenesten og utdanningsinstitusjonene for tannhelsepersonell) hvor man ved hjelp av et kommunikasjonsprogram kan sende henvisninger og epikrise, med kobling mot journalsystem, hvor man også skal kunne legge ved bilder. Videre ønskes det et system hvor forskjellige aktører i tannhelsetjenesten skal kunne kommunisere på en sikker måte seg i mellom, også på tvers av fylkesgrensene, for å kunne søke mer ekspertise eller diskutere vanskelige kasus eller uklare tilfeller. En felles webside som presenterer TkNN og distribuerer aktuell informasjon til allmennheten, er på plass (www.tannhelsetjenesten.no). Tanken er å bruke denne nettsiden som utgangspunkt når kommunikasjonsnettet skal etableres. Hensikten med prosjektet er altså å utrede hvilken teknologi som bør tas i bruk samt hvilke organisatoriske utfordringer man står over for, og deretter anbefale hva som er den beste løsningen i forhold til kostnad.

2 Eier, kunde og andre interessenter

2.1 Eier

Prosjektet er initiert og eid av Den offentlige tannhelsetjenesten i Troms.

2.2 Kunde

Kunden er Den offentlige tannhelsetjenesten i Troms.

2.3 Andre interessenter

Bidragsytere og sentrale samarbeidspartnere er Nasjonalt senter for telemedisin ved Universitetssykehuset Nord-Norge.

3 Brukere

3.1 Brukere av systemet

Alle offentlige og private tannhelsearbeidere i Nordland, Troms og Finnmark, både allmenntannleger, spesialister, tannpleiere, tannlegesekretærer og administrativt ansatte, samt kompetansesenteret for Nord-Norge, vil være brukere av tjenesten.

3.2 Brukerprioritet

Brukerne kan deles inn i forskjellige brukergrupper avhengig av fagområde, for eksempel: Allmenntannlege, Kjeveortoped osv., dvs. undergrupper med forskjellige tilgangsrettigheter.

3.3 Brukermedvirkning

Et utvalg av brukere deltok i prosjektet ved at de kom med ønsker/krav til hva og hvordan systemet skal/kan brukes. Brukerne som deltar i dette forprosjektet er: Overtannlege Øystein Fredriksen og kjeveortoped Kristin Sandvik. Vi har også fått innspill fra tannhelsepersonell i Sør-Troms.

4 Begrensinger

Dagens nettstruktur for tannhelsearbeidere er en klar utfordring for videre oppbygging av et elektronisk nettverkssamarbeid i regionen. Disse utfordringene går på:

Troms: Alle offentlige tannleger/spesialister er knyttet sammen i et fylkeskommunalt nett og er koblet til journalsystem og felles databaser via terminalserver. De private har i all hovedsak ikke hatt noen organisert tilknytting til et elektronisk nettverk. For de som har skaffet seg en slik tilknytting er det snakk om en direkte internettforbindelse. Journalsystem for privatpraktiserende som benytter elektronisk journal, er i stor grad i dag installert på lokal PC.

Finnmark: I løpet av 2007 vil alle offentlige tannleger/spesialister være knyttet sammen i et fylkeskommunalt nett og koblet direkte mot sentralisert journalsystem med terminalserverløsning mot Internett. Det finnes fibersamband i øst og i Alta/Hammerfest. De største klinikkene har 10 Mbit/s, de mellomste 4 og de minste klinikkene har 2 Mbit/s. Alle klinikkene vil i løpet av året ha tatt i bruk digital røntgen, med Digora som databasesystem. Det arbeides for å etablere tilgang utenfra til sikker sone, med to-trinns autentisering fra bærbare PC-er. For de private er situasjonen den samme som i Troms.

Nordland: Tilknytting av tannklinikker til fylkeskommunalt nett for offentlige tannleger/ spesialister er 70-80% gjennomført i Nordland. I løpet av 2008 vil dette arbeidet være ferdig. Det legges opp til sentraliserte databaser med Opus Dental. Tilgang til e-post og internett vil være via Domino WEB-access. Linjekapasitet vil i hovedsak være 2 Mbit/s, - med unntak av kompetanse-senteret som er tilknyttet fiber og dermed større båndbredde. For digital røntgen benyttes Dimaxis, som til nå har blitt etablert i Sør-Helgeland og for kompetansesenteret. Det anvendes mye digitale pasientfoto, som hittil har blitt lagret i programvaren FotoStation. For de private er situasjonen den samme som i Troms.

En terminalserverløsning er bygd på prinsippet om at det ikke skal foregå lokal prosessering, dataoverføring eller datalagring på PC, men at alle slike funksjoner er lagt til sentrale servere. Kun oppdatert skjermbilde – og ikke data – overføres til lokal PC. Citrix er et eksempel på en terminalserverløsning.

Som vi ser ovenfor, er de offentlige tannlegene/spesialistene i Troms koblet sammen via fylkeskommunalt nett og får tilgang til journalsystem og felles databaser via terminalserver, mens i Finnmark er dette omvendt, dvs de har tilgang direkte til journalsystem og databaser, mens de bruker terminalserver mot Internett og e-post. I Nordland bruker de en løsning som ikke er så forskjellig fra Finnmark, men i stedet for terminalserver for tilgang til Internett og e-post brukes Domino WEB-access. Med andre ord så er det valgt tre forskjellige løsninger i de tre fylkene. Nordland og Finnmark har tilnærmet like løsninger som mest sannsynlig ikke vil medføre de store problemene. Troms derimot har valgt en løsing som vil være en utfordring å få til å fungere sammen med de andre fylkene. Den mest hensiktsmessige løsningen med tanke på dataoverføring av personsensitive opplysninger er at tannhelsepersonell har direkte tilgang til journalsystem og felles databaser, og med terminalserver mot internett. Dette vil mest sannsynlig også forbedre opplevelsen av bildekvaliteten for digitale bilder lagret i felles databaser og journalsystem.

5 Relevante fakta

5.1 Navnekonvensjoner og definisjoner

Definisjoner av alle viktige ord og uttrykk brukt i prosjektet, samt alle forkortelser.

E-post	- Elektronisk post
E-læring	- Elektronisk læring
IKT	- Informasjons- og kommunikasjonsteknologi
IT	- Informasjonsteknologi
KITH	- Kompetansesenter for IT i helse- og sosialsektoren
LMS	- Learning Management System
NHN	- Norsk Helsenett
NKU	- Nettbasert kompetanseutvikling
NST	- Nasjonalt senter for telemedisin
OFU	- Offentlig forskning og utvikling
PC	- Personal Computer
TkNN	- Tannhelsetjenestens kompetansesenter for Nord-Norge
UNN	- Universitetssykehuset i Nord-Norge
WWW	- World Wide Web

5.2 Løsninger

Systemet skal baseres på internetteknologi for å oppfylle ønsket tilgjengelighet for tjenesten.

5.3 Omgivelser

Systemet skal kunne benyttes av ansatte i privat og offentlig tannhelsetjenesten i regionen. Det forutsettes at disse er knyttet sammen via en sikret kommunikasjonsløsning (se kapittel 8.7).

5.4 Applikasjoner som produktet skal samhandle med

Nedenfor er det beskrevet applikasjoner som ikke er en del av systemet men som systemet må samarbeide med eller ta hensyn til.

Elektronisk pasientjournal:

> I både den offentlige og private tannhelsetjenesten i Norge i dag er det hovedsakelig ett journalsystem som er i bruk, i tillegg til det papirbaserte. Dette er:
>
> Opus Dental: Opus Systemer AS utvikler, selger og supporterer programvare for tannlegebransjen i Norge, Sverige, Danmark og Finland.

Røntgendatabase:

Det er flere typer røntgendatabaser i bruk. Disse er: Digora, Dimaxis, Sidexis m.fl.

Klinisk fotodatabase:

Et fåtall av klinikkene har opprettet egen klinisk fotodatabase. Eksempel på slik database kan være Opus Bildebanken eller FotoStation.

5.5 Annen kommersiell programvare

Adobe Acrobat Standard vurderes å tas i bruk for å lage pdf-filer av henvisninger fra journal-systemet, mens vi venter på at Opus skal støtte standard formater for henvisninger og epikrise.

5.6 Forutsetninger

Det forutsettes at alle parter som skal delta/bruke fagnettet er koblet sammen via en sikret kommunikasjonsløsning, som holder seg innenfor kravene fra Datatilsynet og lovverket.

6 Produktbeskrivelse

6.1 Fagnettets innhold

Fagnett-portalen skal være en inngangsport til tannhelsetjenesten i Nord-Norge. Denne portalen skal bestå av en åpen del som kan nås fra Internett, og en lukket del som kun er tilgjengelig fra innsiden av det sikrede nettet, via sikker pålogging, som nettbank.

Tjenesten skal i den åpne delen gi informasjon til brukere om privat og offentlig tannhelse-tjeneste og kompetansemiljøer i landsdelen. Den lukkede delen skal tilrettelegges for videreutdanning/kursing og prosedyrebeskrivelse/video for brukerne av løsningen. Det skal også opprettes diskusjonsforum i den lukkede løsningen hvor det skal være mulig å diskutere vanskelige kasus. Det er ønskelig at diskusjonene i forumet skal kunne være personsensitive, hvor digitale tannkliniske bilder/røntgenbilder skal være tilgjengelige enten direkte i forumet, eller via en felles database, eller at disse sendes til deltakerne på forhånd. Her kan man, inntil sikre løsninger er på plass, omgå personsensitive data ved at man i diskusjonene ikke nevner direkte personsensitive opplysninger, men heller henviser til data som kun er tilgjengelig for deltakerne i diskusjonen, samt at bildene kun gjøres tilgjengelig for deltakerne i diskusjonene. Dermed er ikke diskusjonene personsensitive.

Tjenesten skal med andre ord være tilrettelagt for:

- Åpen Internettjeneste
    - Med informasjon til pasienter om priser, rettigheter, etc.
    - Med informasjon om tannhelsetjenesten og dens kompetansemiljøer
    - Med informasjon om kurs/videreutdanning og seminarer

- Lukket intranettjeneste
    - Med tilbud om videreutdanning/kurs og seminarer for tannhelsearbeidere. Dette kan være:
        - Bedriftsinterne forelesninger
        - Kurs og utdanningstilbud for alle yrkesgrupper innen tannhelse
        - Plansjer eller presentasjoner over utførelsesprosedyrer innen tannbehandling
        - Prosedyrebeskrivelse/video for eksempel:
            - Operasjon/behandling av vanskelig visdomstann
            - Rotspissamputasjon
            - Blottlegging av hjørnetenner
            - Lukking av antrums-kommunikasjon
            - Klipping av tungebånd
            - Fjerning av operculum (tannkjøttslapp)
            - Kroneforlengelse
            - Oppdekning Hygiene, spesielt ved smittepasienter
            - Røntgenopplæring for assistenter
            - Oppdekning kirurgi
            - Assistering ved visdomstann-operasjon
            - Bruk av odontosurge (brenneapparat)

    - Med muligheter for eget studiesenter med interaktive kurs som kan inneholde:
        - Kursbeskrivelser
        - Læremoduler
        - Forelesninger med multimedia innhold
        - Litteratur
        - Bildematerialer
        - Funksjoner for veiledning
        - Chat/prategruppe
        - Dokumentdeling/samarbeid

    - Med muligheter for forelesninger og tverrfaglige diskusjoner via video-konferanse, hvor video skal kunne lagres og gjøres tilgjengelig for senere bruk
    - Med muligheter for opplasting av tannkliniske bilder/røntgenbilder, også personsensitive
    - Diskusjonsforum
    - Elektronisk veiledning

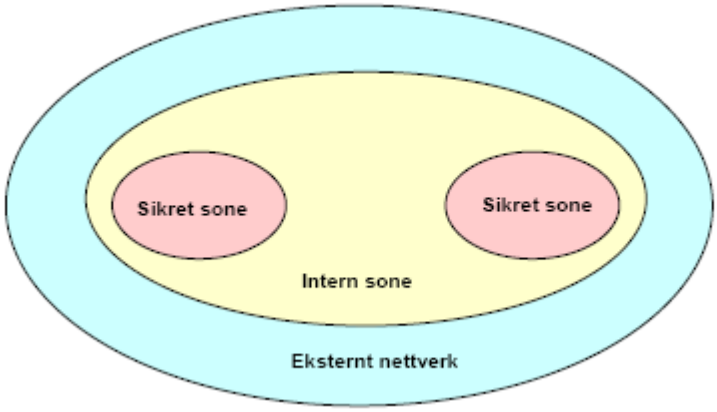
6.2 Brukergrensesnitt

Det er ønskelig at grensesnittet mellom bruker og produkt skal være rent webbasert. I en oppstartsperiode kan det være webbasert i all hovedsak, mens noen deler kan være separate applikasjoner. Meldingsutveksling og en-til-en kommunikasjon (sikker e-post) kan være slike selvstendige applikasjoner på en Microsoft Windows-basert PC.

7 Funksjonelle krav

Det skal være mulig å ha en ”åpen” del av fagnettet som brukes til å formidle informasjon ut via Internett. Denne er eksisterende, men må tilpasses utvidelsen slik at denne kan være inngangsporten til den lukkede delen.
Det må legges til rette for at en person står ansvarlig for å oppdatere denne kontinuerlig, for at siden skal ha den tiltenkte funksjon.

Alle som skal delta i den lukkede delen av fagnettet, skal tilkobles via en sikker løsning som holder seg innenfor kravene til datatilsynet og lovverket (se kapittel 8.7). Det er ønskelig at alle tannleger/spesialister, offentlige og private, samt andre ansatte i tannhelsesektoren skal være koblet sammen via denne lignende løsningen. Datatilsynet har utarbeidet en veiledning for hvordan datanettverk med personopplysninger skal sikres [11]. Disse kravene skal overholdes. Figur 1 er hentet fra denne veilederen, og skisserer hvordan en sikkerhetsarkitektur er inndelt i soner.



Figur 1: Sikkerhetsarkitektur – inndeling i soner

7.1 Funksjonelle krav for ny løsning

Den lukkede delen skal ha sikret pålogging (identifisering og autentisering av bruker) slik at hver bruker identifiseres med en unik id, samt at all bruk skal logges.

Loggene skal ikke kunne forandres i ettertid (slettes fra el.)

En person skal ha ansvaret for at loggene blir sjekket regelmessig og bevart på en sikker måte for framtidig dokumentasjon.

Innenfor den lukkede delen skal det være mulig å finne faglig informasjon, delta i diskusjoner, legge ut/redigere informasjon, dele dokumenter/bilder/video, kommunisere en-til-en via sikker e-post, sende/motta henvisninger og epikrise, planlegge og vurdere bilder i forkant av tverrfaglige møter via videokonferanse, utveksle informasjon, bilder, video, henvisninger, epikriser, e-post - og diskutere disse via nettet på tvers av fylkesgrensene.

Det skal være mulig for deltakere å oppdatere seg faglig via nettbaserte kurs og forelesninger.

All data som skal lagres innenfor den lukkede delen må lagres innenfor et sikkert område av nettet. Eksisterende utstyr som tidligere har vært brukt for lagring av denne type data, og som fortsatt skal ha samme funksjon, må plasseres på et slikt område. Dette gjelder spesielt for private klinikker som ikke har hatt nettilkobling tidligere.

Ingen av dataene innenfor dette området, dvs. bilder, video, osv. må lagres midlertidig på usikret utstyr.

8 Ikke-funksjonelle krav

8.1 Utseende

TkNN's webside ønskes som utgangspunkt for fagnettet, og alle utvidelser (fagnettet) bør følge designet fra denne.

8.2 Brukervennlighet

Fagnettet skal være lett å lære og intuitivt å bruke. Det skal ikke kreves noen ekstra opplæring for bruk, men gode hjelpemenyer bør være tilgjengelig for eventuelle spørsmål om bruk. Det bør også være muligheter for opplæring av brukerne. All tekst i fagnettet skal være på norsk.

8.3 Ytelse og kapasitet

For at fagnettet skal oppleves som effektivitetsfremmende og informasjonsnyttig, må det settes et minimumskrav til maskinvare og nettlinje, samt til logg og bildedatabaser. Systemet skal respondere så raskt at brukere ikke blir irritert over ventetiden, samt at det bør gis beskjed til brukeren når data er under prosessering.
Systemet må også være skalerbart med hensyn til antall samtidige brukere og mengde informasjon som kan legges inn i systemet. I begynnelsen vil prosjektet starte med få brukere, men det skal være muligheter til utvidelse. Potensielt er det 400 tannleger i Nord-Norge, pluss øvrige ansatte i tannhelsetjenesten. Dette må det tas høyde for i valg av løsning.

8.4 Operasjonelle krav

Hvis det er ønskelig at bilder av vanskelige kasus som skal diskuteres i forum skal lagres i en felles database, må det etableres en bildedatabase for slike bilder. I tillegg må det etableres en database for kurs-videoer og -plansjer. Systemet må derfor ta hensyn til en slik etablering.

Drift krever resurser og man må ha profesjonelt personell både for redaktøransvar og teknisk drift.

Drift skal skje på TkNN.

8.5 Vedlikeholdskrav og krav til systemuavhengighet

Det er ønskelig at systemet baserer seg på åpen kildekode i den grad dette er mulig.

Vedlikehold skal utføres av programvareleverandør.

Systemet bør være nettleseruavhengig. Dvs. at løsningen må støtte de vanligste protokoller og nettlesere.

8.6 Sikkerhetskrav

Det skal være mulig å tilgangsbeskytte hele eller deler av fagnettet, og eventuelt nettbaserte kurs og prosedyre-beskrivelse/-videoer.

Ulike deler av tjenesten skal være aksessbeskyttet i forhold til de ulike brukergrupper som defineres. Dette kan for eksempel være:

- Oppdatering av informasjon inkl. opplasting av bilder
- Leserettigheter på innhold, hvem kan lese hva
- Registrering i bruksloggdatabase og bruk av denne.
- Deltakelse i diskusjonsforum og prateforum
- Sending av sikker e-post (meldingsutveksling)
- Publisering av nettbaserte kurs og prosedyrebeskrivelse/videoer

Det skal være mulig å definere ulike brukergrupper, og deretter gi aksess til ulike funksjoner på bakgrunn av disse gruppene.

Det skal på sikt være mulig å diskutere personsensitive data/bilder via diskusjonsgruppene, samt at det skal være mulig å laste opp digitale tannkliniske bilder/røntgenbilder.

Det må opprettes en bruksloggdatabase for fagnettet.

8.7 Juridiske krav

Tannhelsepersonells virksomhet er i likhet med annet helsepersonells virksomhet underlagt en til dels omfattende og streng lovgivning. Viktige hensyn skal ivaretas både overfor helsepersonellet selv, pasientene og myndighetene. Særlig viktig ved bruk av IKT er hensyn knyttet til ivaretakelse av taushetsplikt og spørsmålet om forsvarlig virksomhet.

Autoriserte tannleger, tannhelsesekretærer, tannpleiere og tannteknikere er alle omfattet av helsepersonelloven [1], se § 3 og § 48 w–z.

Bestemmelser om journalføring generelt og elektronisk journal spesielt finnes i journal-forskriften [2].

Helseregisterloven [3] er en særlov under personopplysningsloven [4], og disse stiller ganske likelydende krav til informasjonssikkerhet.

Personopplysningsforskriften [5] påpeker at virksomheter i helsesektoren har meldeplikt til Datatilsynet for all elektronisk behandling av personopplysninger. Den omhandler også krav til fysisk sikring, sikring av konfidensialitet og dokumentasjon.

"Norm for informasjonssikkerhet i helsesektoren" [6] stiller krav som detaljerer og supplerer gjeldende regelverk.
Se også Datatilsynets egen informasjon om meldeplikt eller konsesjon. [7].

For mer detaljert informasjon, se vedlegg 1.

9 Organisatoriske utfordringer

9.1 Bakgrunn for fagnett

Tannhelsetjenestens kompetansesenter for Nord-Norge (TkNN) ble formelt etablert i 2003. TkNN skal blant flere oppgaver også ha en regionfunksjon for Nord-Norge. For å jobbe videre med regionfunksjonen ble det våren 2004 satt ned et regionalt prosjekt som skulle klarlegge hvordan de tre fylkene skulle samarbeide og hva de skulle samarbeide om. Prosjektet fremmet ønske om at det ble etablert et fagnett til nytte og vekst for de tre nordligste fylkene.

I 2006 ble det gjennomført en spørreundersøkelse rettet mot alle tannlegene i Nord-Norge. Det ble bl.a. spurt om behovet for kommunikasjon med bilder og journaldata på nett. Den generelle tilbakemeldingen var at kommunikasjon med bilder og journaldata, samt opplæring via demonstrasjonsvideo var positivt mottatt. Det er også foretatt kvalitativt intervju med en fokusgruppe som besto av tannleger fra distrikt Sør-Troms. Også disse så stort utbytte-potensial i et slikt nettverk. I tillegg har spesialistene som er ansatt ved TkNN, samt tannhelsemiljøet i Nord-Norge uttrykt stort behov for et eget fagnettverk. Det er i det hele tatt stor vilje til å kommunisere på nett. Bruksmulighetene er mange: Opplæringsvideoer, mulighet for å sende sikker e-post; henvisning, epikrise, bilde og journaldata.

9.2 Organisatoriske utfordringer

Selv om entusiasmen synes å være stor, vil nok mange oppleve at bruken av et slikt nettverk vil endre de daglige rutinene, men det kan også være noen som ikke helt ser nytten av et slikt nettverk. Det kan nok knytte seg en del utfordringer til bruk av et slikt fagnett.

1. I regionen varierer størrelse på tannklinikkene, alt fra en-mannsklinikker til klinikker med 10 – 15 ansatte. Det kan være grunn til å tro at de større klinikkene allerede har et faglig godt samarbeid, og at de ut fra dette ikke ser den samme nytten. Samtidig viser undersøkelsen fra 2006 at tannleger som jobber i større miljøer har en

tilbøyelighet til å søke enda mer kompetanse, noe som kan bety at fagnett blir et supplement for de eksisterende samarbeidsstrukturene.

2. Våre erfaringer er også at noen distrikt i stor grad bruker hverandres interne kompetanse i forbindelse med diagnoser og den kliniske behandlingen.

3. Det er også grunn til å nevne at innenfor enkelte fagmiljø er det i dag allerede etablerte elektroniske nettverk hvor faglige problemstillinger blir utredet og diskutert.

4. Det kan også være en sammenheng mellom behov/mulig bruk av et spesialist-nettverk og erfaring som tannlege. En tannlege som har lang erfaring vil kanskje bruke et slikt nettsted mindre enn en med noe mindre klinisk erfaring.

5. I dag er kjennskapen til og erfaringen med å jobbe elektronisk varierende. Det er grunn til å tro at terskelen for å ta dette nye kommunikasjonsverktøyet i bruk blir noe mindre for de tannlegene som har stor erfaring med å jobbe elektronisk, som å bruke ulike søkemotorer, konsultere kollegaer via e- post, kjennskap til å håndtere digitale bilder m.m. Det er også grunn til å tro at tannleger som ikke har denne type erfaring ikke uten videre vil benytte seg av et fagnettverk.

6. Å søke råd/kollegakonsultasjoner kan for enkelte oppleves som en barriere. Det kan være at enkelte synes spørsmålene de stiller er for elementære og er redd for å fremstå som lite kompetent innenfor sitt fagområde. Det er nærliggende å tro at de som er forholdsvis nyutdannet har en annen tilnærming til dette, og at de via sin utdannelse har lært denne pedagogiske metoden å kjenne via sin utdannings-institusjon.

7. I spørreundersøkelsen som ble gjennomført i 2006 ble det bl.a. spurt om hvilken betydning kommunikasjon med bilder og journaldata vil ha for den enkelte. Blant tannleger med over 20 års erfaring svarte 53 % at det vil ha stor/svært stor betydning, mens av de som har mindre enn et års erfaring svarte 88 % at det har stor/svært stor betydning.

8. I Nord-Norge er det stor tannlegemangel og stabiliteten har vært dårlig. Det er mange nyutdannede tannleger, og det er grunn til å tro at de fleste nye vil bruke et fagnett. Man kan også antyde at et faglig kommunikasjonsnettverk kan virke stabiliserende på tannlegene. Et faglig fellesskap og faglige utfordringer viser seg å være viktig for nyutdannede tannleger.

9.3 Utbygging av elektronisk infrastruktur

Utbyggingstakt for elektronisk infrastruktur på bredbånd, og utnyttelse av denne i tannhelse-tjenesten, har vært noe forskjellig i de tre fylkene.

- Finnmark har samlet pasientdata for offentlig tannhelsetjeneste i sentraliserte lagringsdatabaser i Vadsø, og er i gang med bredbåndsutbygging over hele fylket.

- I Troms har alle offentlige tannklinikker blitt tilknyttet infrastruktur fra Bredbåndsfylket Troms, og lagrer data i sentral database i Tromsø. TkNN er i dag en del av dette driftsmiljøet.

- Nordland har hatt mange offentlige tannklinikker spredt rundt i fylket, med lokal datalagring, og fylket har kommet noe kortere i utbygging av bredbånd enn de to andre fylkene. I løpet av 2008 vil imidlertid alle offentlige klinikkene være knyttet sammen i et elektronisk datanett.

Privat tannhelsetjeneste har i alle de tre fylkene blitt basert på lokal datalagring i klinikken, og i utgangspunktet uten at det finnes elektroniske kommunikasjonsveier tilgjengelig. Disse er derfor i mindre grad vant til å benytte kommunikasjonsteknologi som verktøy.

9.4 Fokus på implementering

En av forutsetningene for å lykkes med fagnett er selve implementeringen. Det er flere faktorer som er viktig:

1. Informasjon om bruk og funksjonalitet. Når forprosjektet er ferdig må det fokuseres på intern informasjon om fagnett, bruksområder og funksjonalitet.

2. Opplæring. Det bør prioriteres å lage et strukturert opplæringsprogram. De fleste tannlegene jobber klinisk hver dag og har mye å gjøre. ”Nybrottsarbeid” som dette kan bli nedprioritert og det kan bli vanskelig å komme i gang. De tannleger som har minst erfaring med bruk av IKT vil nok være de som har størst behov for en praktisk tilnærming: hvordan komme i gang.

3. Det bør vurderes om det skal utpekes et pilotdistrikt sammen med TkNN

Behovet for konsultasjon og faglig oppdatering vil være ulikt, og tannlegene vil nok også oppleve behovet varierende. Men, innenfor odontologi som fag er det en fortløpende utvikling, og det er nok en forventning om at tannlegene oppdaterer seg i takt med denne utviklingen. Som nevnt er også utbyggingen av elektronisk infrastruktur varierende i de nordligste fylkene. I dag er det heller ikke alle som har tilgang til digitalt fotoutstyr, men på sikt vil nok dette jevne seg ut. For at tannleger i nord skal bli aktive brukere av nettverket vil det være avgjørende at brukergrensesnittet er intuitivt, samt at implementeringen blir godt gjennomarbeidet.

10 Presentasjon av sikrede nettverksløsninger

10.1 Norsk Helsenett

Det har fra statens side de seneste år blitt satset store ressurser og økonomiske midler innenfor helse- og sosialsektoren for et landsdekkende, sikret kommunikasjonsnett for tele- og datatjenester: Norsk Helsenett. Her er det lagt til rette for tilknytning av, først og fremst sykehus og legekontorer, og etter hvert helse- og sosialinstitusjoner. Dette forprosjektet har vurdert muligheten for at landsdelens private og offentlige tannleger tilknyttes samme nett.

Norsk Helsenett eies av de fem helseregionene. Nettet skal være en felles samhandlings-arena for aktører innenfor helse- og sosialsektoren.

Oppbygging av sikret infrastruktur basert på internett-teknologi har kommet relativt langt innenfor helsesektoren i de fleste deler av landet. Det gir brukeren en sikret tilgang til et standardisert kommunikasjonsnett med fordelaktig prising av infrastruktur. Ensartede tekniske løsninger gir forenklet drift og mindre problemer.

Nettet anvendes i hovedsak for sikret kommunikasjon mellom legekontor og sykehus, med knytninger mot andre samarbeidspartnere og tilgang ut til åpne nett. Det er i dag svært få tannklinikker tilkoplet Norsk Helsenett.

I tillegg til infrastruktur er det etablert et relativt beskjedent sett med tilgjengelige basis-tjenester. Dette dreier seg om for eksempel

- Adresseregister
- Betalingsterminaler
- Bransjenormen og Kommuneveileder
- Elektronisk dokumentutveksling - EDI
- Microsoft lisensavtale
- E-post og Internett
- Ulike videokonferanseløsninger, bl.a. IP-basert internt i helsenettet.
- Sikkerhetsoppdateringer

Norsk Helsenett vil ikke lage egne tjenester for tannhelse, men er åpen for at andre tjenestetilbydere kan tilby sine tjenester gjennom nettet. Tjenesteytere i helsenett i dag er i hovedsak sykehusene. Det vil dermed være opp til tannhelsetjenesten selv å finne nyttige tjenesteleverandører for oss og få etablert disse i nettet.

Norsk Helsenett er positiv til et eventuelt samarbeid med tannhelsetjenesten, men påpeker viktigheten av å etablere de standarder som trengs for å kommunisere i nettet, og få disse integrert i EPJ-systemet. Det er liten interesse for å lage overgangsløsninger før dette er på plass.

Tilknytning av tannklinikker til Norsk Helsenett forutsetter at en ikke har annen nett-tilknytning. For offentlige klinikker som i dag er tilknyttet fylkeskommunale nett vil dette være en utfordring, som en sammen med NHN må finne løsning for.

10.2 Norsk Tannhelsenett

Informasjonen her er hentet fra [12].

I samarbeid med to aktører (Emma EDB og Aspector) innen informasjons- og kommunikasjonsteknologi i helsesektoren, tilbyr Opus Systemer AS et landsdekkende og sikkert IT-nettverk for dentalbransjen. Norsk Tannhelsenett er den eneste løsningen med full integrasjon mot Opus Dental, og nettverket inneholder følgende funksjoner:

- Elektronisk meldingsutveksling
- Internett

- E-post
- SMS
- Hjemmekontor
- Reiseløsning
- Fjernsupport fra Opus Systemer AS
- Automatisk oppdatering av Opus Dental
- Backup etter avtale

Installasjon og pris pr. jan. 2007: Etablering/oppstartskostnaden er fra kr. 9.900.- til 14.100.- pr. klinikk. Dette inkluderer leie av kommunikasjonsutstyr, antivirus, brannmurer, etablering av internettlinje, e-post, SMS og tilknytning til EDI meldingsutvekslingsserver. Den løpende månedlige kostnaden inkluderer en bredbåndstilknytning og koster 1.210 kr eks. mva.

Sikkerheten er i henhold til datatilsynets og helsetilsynets krav og normer.

Hvis tannklinikken pr. i dag er tilknyttet en annen nettleverandør, er Opus behjelpelig med konvertering. Når det gjelder fylkeskommunale tilkoblinger, er ikke disse ifølge Opus Systemer noe problem å koble opp mot dette nettet.

10.3 Andre løsninger

Norsk Dentalnett [17] er en annen løsning som ved hjelp av sikrede linjer kan koble sammen landets tannlegeklinikker i et stort nettverk. Løsningen er utviklet av Medic IT AS, og tilbyr følgende basistjenester:

- Internett og epost i terminalvindu for å skille klinikkens pasientdata fra normal internettbruk.
- Kommunikasjonssystem for å sende og motta henvisninger og epikriser digitalt, rett fra ditt journalsystem.
- Tannlegeforum for å utveksle erfaringer, spørsmål og synspunkt i et lukket fagnett.
- Helautomatisk backup av klinikkens journalsystem gjennom samme nettverk.

Det er også mulig å **leie egne linjer** fra nettleverandører som for eksempel Telenor, Ventelo og NextGenTel, men dette forutsetter som regel at man da må ha en del teknisk innsikt i forhold til sikkerhet, som ofte igjen krever en egen IT-ansatt for å ivareta drift. Det er sikkert også mulig å kjøpe disse tjenestene fra flere nettleverandører, men vi har ikke sjekket dette videre.

11 Presentasjon av fagnettløsninger

Målet med et fagnett er å knytte profesjoner sammen via et intranett. Gjennom å etablere et fagnettverk mellom de ulike gruppene ved landsdelens, og etter hvert landets tannhelse-klinikker, også privatpraktiserende, kan man kanskje bedre rekrutteringen til faget, samt at det vil knytte fagfolkene tettere sammen, noe som er spesielt viktig for distriktene. Det stilles stadig nye og økende krav til omfanget av og kvaliteten på de diagnostiske tjenestene. Nettverket skal legge til rette for fagutvikling, kompetanseoverføring, forskning og kvalitetssikring og bidra til raskere og mer rasjonell distribusjon og rekvirering av informasjon og faglig kompetanse. Nettverket skal være et verktøy som setter de ulike tannspesialiteter i

stand til samarbeid og videreutvikling av det eksisterende fagmiljø, samt gjøre avstander mellom klinikker ” virtuelt kortere”.

Dette er en presentasjon av mulige løsninger for fagnett, til bruk i den offentlige og private tannhelsetjenesten i Nord-Norge. Vi har ikke testet de forskjellige løsningene, men har samlet informasjon fra websider og gjennom samtaler med representanter for de forskjellige løsningene. Vi har samlet inn opplysninger om pris, linker til mer informasjon og annen informasjon vi mener kan være relevant der det har vært tilgjengelig. Vi har foreløpig tatt utgangspunkt i 100 brukere av fagnettet når det gjelder prisinformasjon.

11.1 Classfronter

Dette er et program for nettbasert undervisning som leveres av selskapet Fronter. De retter seg for en stor del mot undervisningssektoren, men har også løsninger som egner seg for bedrifter, organisasjoner etc. I Tromsø er Ibis IKT forhandler for Fronter.

Løsningene deres inkluderer arkiv for oppbevaring av filer, meldinger, diskusjonene i diskusjonsforum.

Classfronter har i det siste vært svært utbredt, blant annet i utdanning av helsepersonell. For en del yngre personell vil derfor løsningen være kjent.

Fronter er også etablert i flere land, deriblant Sverige, Finland og Storbritannia.

Denne løsningen ivaretar ikke informasjonssikkerheten godt nok og dermed egner den seg ikke for diskusjoner av personsensitiv data.

Kostnadsoverslag fra Ibis IKT:
Strukturering av prising, Fronter - liten bedrift:

100 lisenser (en bruker per lisens)	à kr 338	= 33800,- (årlig)
Drift av installasjon		= 20000,- (årlig)
Årlig kostnad		= 53800,- (eks.mva)

Oppbygging av struktur med registrering av brukere - engangskostnad = 5000,- (eks. mva)
Innrømmelse - inntil 200 lisenser til samme pris!

Kursrekke:
Administrator av Fronter - obligatorisk for å få teknisk support.
2 dager à 8.500,- = 17.500,- (ikke mva. pliktig)
Brukerkurs på Fronter - superbrukere i kommunene. Maks 20 deltakere pr kurs (hver sin pc)
2 dager à 8.500,- = 17.500,-

Kurs avholdt på Ibis - inntil 13 deltakere per kursdag.
Lisens og drift faktureres av Fronter mens strukturering og kurs faktureres av Ibis IKT as.
Grunnskoler har hatt god nytte av direkte brukersupport fra Ibis IKT as og spart masse tid.
En slik brukersupport for fagnettet settes til årlig kr. 10.000,- (hvis ønskelig) - da kan den enkelte bruker ta direktekontakt med Ibis IKT as for å få brukerstøtte.

Websider: www.fronter.no & www.ibisikt.no

11.2 It’s learning

I likhet med Classfronter er It’s Learning et e-læringssystem, hovedsakelig beregnet på undervisning. Likevel vil funksjonaliteten i løsningen være godt egnet for et fagnett. Systemet har all den funksjonaliteten som kreves, men egner seg ikke for personsensitive diskusjoner.

It’s Learning har over 450 000 brukere fordelt på Norge, Sverige, Danmark, England, Tyskland og Nederland.

Kostnadsoverslag fra It’s Learning:

451 kr/bruker per år (inkluderer da også drift av servere og 1GB lagringsplass)

It’s Learning anbefaler også at de som har et sentralt ansvar for løsningen har en minimumsopplæring. Normalt vil dette inkludere både grunnopplæring, og superbruker-/ administrator-sertifisering for ca 15.000 kroner - litt avhengig av hvor mange som deltar. Denne opplæringen kan også gjennomføres som nettbasert opplæring, og gir tilgang til deres supporttjeneste uten tilleggskostnader.

Webside: http://www.itsolutions.no/

11.3 Atutor

Dette er en løsning som bruker fri kildekode. Atutor bruker GNU General Public License (GPL), som kort oppsummert betyr at man gratis kan laste ned, bruke og endre program-varen, men at alle endringer må følge samme lisens.

Denne løsningen gir store muligheter for tilpassing, men det krever teknisk kompetanse fra de som skal drive dette.

Løsningen kan antageligvis tilpasses slik at man kan diskutere personsensitiv data, men det krever utvikling.

Kostnadsoverslag: Atutor kan lastes ned gratis. Dette krever at man har folk som kan drive dette selv, så det vil kreve en god del resurser for å tilpasse og drifte løsningen. Ellers kan man leie support for $650, og hosting fra $650 dollar.

Webside: www.atutor.ca

11.4 Helsekompetanse.no

Helsekompetanse.no er primært en portal for nettbaserte utdanningstilbud innen helsesektoren. I tillegg til dette tilbys det muligheter for fagnettløsninger.

Helsekompetanse tilbys av Nasjonalt senter for telemedisin. Denne løsningen benytter Atutor som grunnlag.

Helsekompetanse.no brukes allerede til å levere en lang rekke fagnett.

Kostnadsoverslag:

Alle priser er eks. mva.

Startpakke 1: etablering og brukerstøtte ved første oppstart av kurs eller fagnett, pris pr. 01.01.2007 Kr. 20 000

Dette er en pakke som inkluderer:
- Spesifisering av innhold
- oppretting av kursrom / fagnett med verktøy
- personlig banner for kursrom / fagnett
- tildeling av administratorrettigheter
- opplæring i bruk av verktøyet til fagansvarlig
- support

Etter kursing vil kunde selv kunne legge inn innhold i fagnett/kursrom og administrere og styre den daglige bruk av fagnettet/kurset.

Ut over dette vil det beregnes et timehonorar for ytterligere utvikling av læringsinnhold, samt også for opplæring i bruk av fagnettet til deltagere.

Webside: www.helsekompetanse.no

Det er også mulig å leie kompetanse fra NST/NKU for hjelp til å sette opp denne løsningen og eventuelt videreutvikle den i et lukket "tannhelsenett", men da må det avtales pris og hvilken løsning man ønsker med NST/NKU.

11.5 Well Community

Denne løsningen er ikke ferdig utviklet og det er Well Diagnostics som har planer for en slik løsning. Løsningen er beregnet å være et sikkert fagnett hvor personsensitive data kan diskuteres, personsensitive bilder kan lastes opp i disse forumene, sikker chat, osv. Løsningen skal kunne kombineres med allerede eksisterende løsninger som **Well Communicator** (meldingstjenester), **Well Arena** og **Well Multimedia** (publikumstjenester, multimedia, web og fagnett). Dette er til nå den eneste sikrede løsningen vi har kommet over for diskusjonsgrupper som er planlagt å kunne håndtere personsensitive data/bilder. Mer informasjon om deres eksisterende systemer finnes på [13]

Markedet for denne typen løsninger er begrenset, så for å få utviklet denne løsningen ferdig er Well Diagnostics avhengig av økonomisk støtte i form av utviklings-/forskningsmidler eller en direkte økonomisk kompensasjon for ferdigutvikling.
(Didrik Widding på Well Diagnostics har gitt oss denne informasjonen.)

11.6 Visma Unique

Informasjonen her er funnet på [14].

Visma leverer samhandlingsløsninger og publikumsløsninger for sikker kommunikasjon mellom helsepersonell og pasienter via Internett og SMS, og er en viktig del deres tilbud til helseforetak.

Unique Link
Unique Link er en komplett løsning for elektronisk samhandling som tilfredsstiller strenge krav til sikker utveksling og behandling av personsensitiv informasjon. Unique Link kombinerer EDI og moderne integrasjoner basert på XML og Web Services på en måte som gjør helseinstitusjoner i stand til å automatisere store deler av dagens manuelle arbeidsflyt.

MedAxess
MedAxess er en komplett løsning for sikker kommunikasjon mellom helsepersonell og pasienter via Internett og SMS.

Portalløsningen
Portalløsningen fra Visma er en publiseringsløsning og virksomhetsportal for håndtering av bedriftens behov for effektiv og kvalitetssikret informasjonsflyt. Den kan bygges ut gradvis med moduler og tredjepartsløsninger etter behov, og omfatter Internett-, intranett- og ekstranettfunksjonalitet.

11.7 Unident – C-takt LINK

C-takt LINK [16] er ikke en fagnettløsning, men et kommunikasjonsprogram laget for tannhelsetjenesten. Dette er et program som er laget for å kunne kommunisere elektronisk, inklusiv bildebasert kommunikasjon, mellom tannlege, spesialist, trygdekontor, tanntekniker. C-takt Link er utformet i samarbeid med allmenntannleger, spesialister og tannteknikere, det inneholder alle de funksjoner som behøves for å kunne tegne, terapiplanlegge og diskutere direkte i bildene uten å ødelegge originalen. Programmet har koblinger til de vanligste journal- og røntgenprogrammene på markedet. Du kan arbeide i ditt journalsystem og på en enkel måte overføre informasjonen inn i C-takt Link. Løsningen er sikker, men vi har ikke vurdert om den tilfredsstiller kravene fra bl.a. Datatilsynet, se vedlegg 1.

12 Drøfting og tilrådninger

Flere i prosjektgruppen har vært involvert i et nasjonalt forprosjekt for utredning av behov og muligheter for elektronisk kommunikasjon i tannhelsetjenesten [18]. I denne rapporten foreslås det at fylkestannlegene inngår en avtale om et landsomfattende IKT-samarbeid og at tannlegeforeningen inviteres som medlem for å sikre medvirkning av den private tannhelsetjenesten. Det foreslås videre at det i første omgang iverksettes arbeid med to konkrete forslag:

1. Etablering av standarder for elektronisk samhandling innenfor tannhelse
2. Forprosjekt for å utrede muligheten for et felles odontologisk fagnett.

Vi støtter fullt ut forslagene i den nasjonale rapporten. Punkt 1 i de konkrete forslagene er viktig å jobbe for på nasjonalt plan, men når det gjelder punkt 2, så er utredningen med denne rapporten allerede gjort i regi av TkNN. Fagnettet som foreslås er en stor utfordring å bygge opp, og det kan være en fordel å starte i mindre skala enn på landsbasis, for å finpusse både tekologisk og faglig løsning. Dermed foreslår vi som en fortsettelse av den nasjonale utredningen, at vi i første omgang starter en pilot for utprøving av et felles odontologisk fagnett i Nordland, Troms og Finnmark, med gradvis utvidelse til resten av landet. Et godt argument for at dette skal starte i Nord-Norge, er at TkNN allerede har en del erfaring med bruk av telemedisin og E-læring ut fra det gjennomførte og vellykkede prosjektet Ortopol@r [19], samt det etablerte samarbeidet med NST i Tromsø, som har mange års erfaring fra lignende løsninger i helsevesenet. Denne erfaringen bør utnyttes.

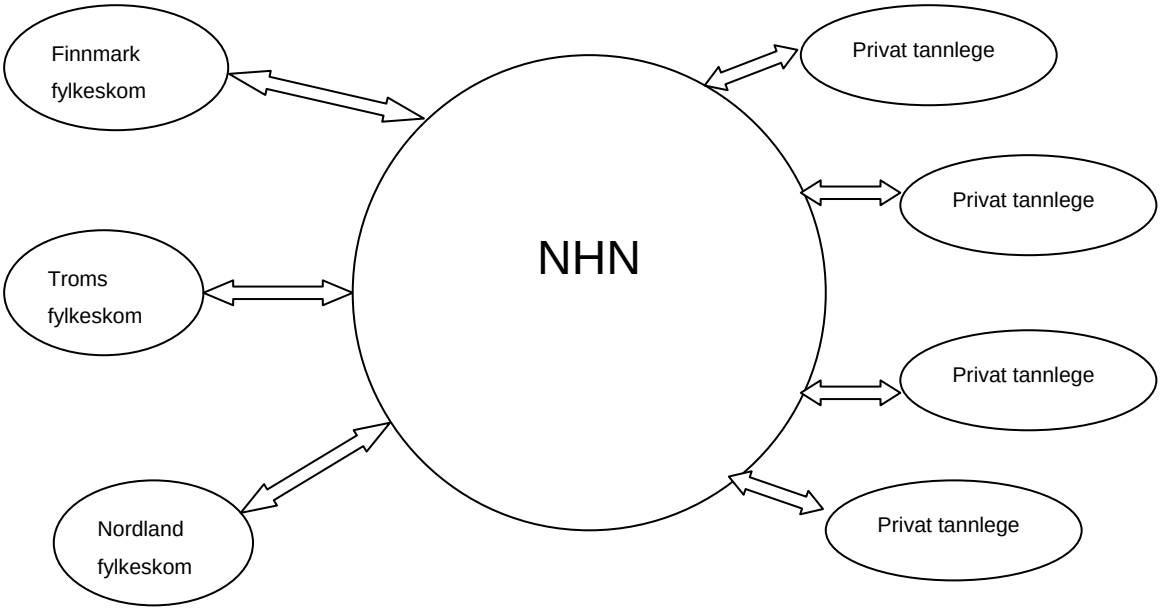
12.1 Nettverksløsninger

I kapittel 10 har vi lagt fram forskjellige teknologiske løsninger for å koble sammen tannlegekontorene i Nord-Norge. Alle disse løsningene er sikkerhetsmessig og tekologisk gode, men for en pilot og mulig framtidig løsning har vi kommet fram til at Norsk Helsenett vil være den mest fordelaktige nettverksløsningen. Denne løsningen blir brukt av Helsevesenet i Norge pr. i dag, og de har dermed erfaring og tjenester som tannhelsetjenesten også kan dra nytte av. I og med at dette er en stor aktør innen helse og etter hvert kommunesektoren, vil alle aktører som skal kommunisere med disse, for eksempel NAV, være nødt til å forholde seg til NHN. Slike aktører vil også være aktuelle for tannhelsetjenesten.

Figur 2 på neste side, skisserer løsningen som vi anbefaler at pilotprosjektet bør ta i bruk. Her ønsker vi en løsning med NHN som nett- og tjenesteleverandør, hvor de fylkeskommunale tannlegene som allerede er koplet sammen i fylkeskommunale datanett i Nordland, Troms og Finnmark, får en tilkobling til NHN. For de private tannlegekontorene vil vi anbefale en direkte tilkobling til NHN som eneste nettløsning, på samme måte som legekontorene i dag er tilknyttet. NHN har som krav at en ved tilknytning til Helsenett ikke samtidig skal være tilkoplet andre nett. I samarbeid med NHN må en søke å finne løsning på denne utfordringen for den fylkeskommunale tannhelsetjenesten, som i dag er tilkoplet fylkeskommunale datanett.

12.2 Fagnettløsning og annen programvare

I kapittel 11 presenters forskjellige fagnett- og programvareløsninger. I og med at det pr. i dag ikke finnes tilgjengelige fagnettløsninger som er sikre nok til at personsensitiv data kan presenteres, har vi kommet fram til at Helsekompetanse.no kan brukes i et pilotprosjekt som en fagnettløsning, se kapittel 11, i påvente at en sikker nok løsning utvikles. Her kan man legge til rette for tjenestene nevnt i kapittel 6, men da med anonymiserte data i første omgang. Dette vil etter vår vurdering være den beste og billigste løsningen for disse tjenestene. Videre anbefales Well Communicator som meldingsutveksler hvor person-sensitive data kan sendes til deltakere i diskusjonsgrupper. Denne løsningen anbefales også til bruk for sending av henvisninger og epikrise i PDF-format, i påvente av at journal-leverandør har utviklet i henhold til standarder for slik kommunikasjon. Dette anbefales for å få testet en slik tjeneste i pilotprosjektet.



Figur 2: Foreslått nettverksstruktur for den fylkeskommunale og private tannhelsetjenesten.

12.3 Økonomi- og tidsestimat for pilotprosjekt

Et pilotprosjekt for oppbygging av infrastruktur og fagnettløsning for tannhelsetjenesten, i første omgang i Nord-Norge, men som etter hvert kan utvides til resten av landet, vil ta tid. Selv om vi med denne rapporten har gjort mye av utredningen, vil det bl.a. være nødvendig med en full risikoanalyse i starten av et pilotprosjekt. Eksperter fra NST på dette området bruker minimum 80 timer på en slik analyse, som forutsetter at all nødvendig informasjon er tilgjengelig. Det vil også ta en del tid før man har fått koblet alle involverte aktører til Norsk Helsenett. Det må beregnes tid til etablering og oppbygging av fagnettet, samt basis innhold i dette, da med særlig tanke på prosedyrebeskrivelse/video. Mye av dette kan gjøres parallelt med at infrastruktur kommer på plass. Det må også beregnes tid til etablering og testing av annen programvare som skal brukes, for eksempel Well Communicator og oppsett av programvare for utskrift av henvisninger til PDF-filer. Det er planlagt med ca. 40 spesialister/tannleger som deltakere i pilotprosjektet.

For å få tid til alt dette, har vi kommet fram til at et grovt tidsestimat for å gjennomføre et pilotprosjekt av denne størrelsen, er på ca. 2 år, hvor oppstart kan skje i løpet av høsten 2007.

Dette vil selvfølgelig medføre en del kostnader. En grov estimering ut fra tidsbruk for innleid prosjektledelse og nødvendige prosjektmedarbeidere, eventuell tilpassing av programvare, etablering av fagnett, samt hjelp til oppbygging av innhold til fagnett osv, har gitt som resultat at dette vil koste ca. 1,5 millioner kroner pr. år. Den totale kostnaden vil da være i størrelsesorden ca. 3 millioner kroner for hele pilotperioden, men bør utredes mer nøyaktig før eventuell oppstart av et pilotprosjekt.

Referanser

[1] Lov om helsepersonell m.v. (Helsepersonelloven)
http://www.lovdata.no/cgi-wift/wiftldles?doc=/usr/www/lovdata/all/nl-19990702-064.html&emne=helsepersonelloven&

[2] Forskrift om pasientjournal (Journalforskriften)
http://www.lovdata.no/for/sf/ho/ho-20001221-1385.html

[3] Lov om helseregistre og behandling av helseopplysninger (Helseregisterloven)
http://www.lovdata.no/cgi-wift/wiftldles?doc=/usr/www/lovdata/all/nl-20010518-024.html&emne=helseregisterloven&

[4] Lov om behandling av personopplysninger (Personopplysningsloven)
http://www.lovdata.no/cgi-wift/wiftldles?doc=/usr/www/lovdata/all/nl-20000414-031.html&emne=personopplysningsloven&

[5] Forskrift om behandling av personopplysninger (Personopplysningsforskriften)
http://www.lovdata.no/for/sf/fa/fa-20001215-1265.html

[6] ”Bransjenormen” – Norm for informasjonssikkerhet i helsesektoren
http://www.shdir.no/samspill/informasjonssikkerhet/norm_for_informasjonssikkerhet_i_helsesektoren_53069

[7] Datatilsynet: ”Melde eller søke konsesjon?”
http://www.datatilsynet.no/templates/article____215.aspx

[8] NST: ”Enkel veiledning for gjennomføring av risikovurdering”
http://www.telemed.no/sikkerhet - se under avsnittet Risikoanalyse midt på siden, der ligger veiledning og en enkel rapportmal

[9] Datatilsynet: ”Risikovurdering av informasjonssystem”
http://www.datatilsynet.no/templates/article____888.aspx

[10] KITH: ”Risikoanalyse. Metodegrunnlag og bakgrunnsinformasjon”
http://www.kith.no/templates/kith_WebPage____637.aspx

[11] Datatilsynet: Veiledning i informasjonssikkerhet
http://www.datatilsynet.no/upload/Dokumenter/infosik/veiledere/tv202_2005_1.pdf

[12] Norsk Tannhelsenett:
http://www.norsktannhelsenett.no/index.php?option=com_frontpage&Itemid=1

[13] Well Diagnostics:
http://well.no/index.php?option=com_content&task=view&id=23&Itemid=20

[14] Visma Unique:
http://visma.no/index.asp?strurl=//applications/system/publish/view/showObject.asp?infoobjectid=1000967

[15] H. Høvik, E. K. Christiansen, E. Henriksen, L. E. Nohr, E. Skipnes: Når tannfeen ”goes online” Bruk av informasjons- og kommunikasjonsteknologi i tannhelsetjenesten. Nor Tannlegeforen Tid 2004; 114: 276 – 82 http://www.tannlegetidende.no/pls/dntt/pa_dtdm.xpnd?vp_seks_id=96572&b_start=1

[16] Uident c-tact LINK: http://www.unident.no/extra/pod/?id=85&module_instance=1&action=pod_show

[17] Norsk Dentalnett: http://www.medic-it.no/nyheter_detail.asp?iid=53

[18] @tann.no: Rapport fra Forprosjekt for utredning av behov og muligheter for elektronisk kommunikasjon i tannhelsetjenesten.

[19] Oropolar@: http://www.telemed.no/index.php?id=73354

Vedlegg 1: Informasjonssikkerhet og risiko

Lovgivingen stiller krav om at det gjennom planlagte og systematiske tiltak skal sørges for tilfredsstillende informasjonssikkerhet ved behandling av personopplysninger. Informasjonssystemet og sikkerhetstiltakene skal dokumenteres, og den enkelte virksomhet skal etablere et internt styringssystem for informasjonssikkerhet og ha rutiner for jevnlig sikkerhetsrevisjon. I dette inngår også gjennomføring av risikovurderinger. Risikovurdering skal gjentas med jevne mellomrom, og skal alltid gjøres ved endring i behandlingen av personopplysninger.

Virksomheter i helsesektoren har meldeplikt til Datatilsynet for all elektronisk behandling av personopplysninger, og ved endringer i slik behandling. Meldingen skal bekrefte at virksomheten har sikkerhetsdokumentasjon, har utført risikovurdering og har et opplegg for systemrevisjoner, vedlikehold og versjonskontroll. Melding skal sendes til Datatilsynet senest 30 dager før systemet tas i bruk. Ved et eventuelt tilsyn vil Datatilsynet be om å få se tilgjengelig dokumentasjon, inkludert rapport fra risikovurdering.

Dette vedlegget beskriver hovedtrekkene i gjennomføring av risikovurdering (avsnitt 1.3). Noen forslag til mulige trusler er tatt med i avsnitt 1.4. Men først oppsummeres juridisk rammeverk og generelle krav til informasjonssikkerhet. [15] tar opp temaet innenfor tannhelse.

1.1. Juridisk rammeverk

Autoriserte tannleger, tannhelsesekretærer, tannpleiere og tannteknikere er alle omfattet av helsepersonelloven [1], se § 3 og § 48 w–z.

Et viktig kapittel i helsepersonelloven er kap. 5 om taushetsplikt. Utgangspunktet slås fast i § 21 der det heter at *"Helsepersonell skal hindre at andre får adgang eller kjennskap til opplysninger om folks legems- eller sykdomsforhold eller andre personlige forhold som de får vite om i egenskap av å være helsepersonell."* Det å hindre slik adgang innebærer både det å overholde taushetsplikt og å oppbevare journal og annen dokumentasjon på en sikker måte. Det siste er særlig aktuelt i forbindelse med innføring av elektroniske journaler og elektronisk formidling av helseopplysninger. Helsepersonellovens § 46 slår fast at pasientjournal kan føres elektronisk. Bestemmelser om journalføring generelt og elektronisk journal spesielt finnes i journalforskriften [2].

Helseregisterloven [3] og personopplysningsloven [4] stiller ganske likelydende krav til informasjonssikkerhet. Ett av kravene er at det gjennom planlagte og systematiske tiltak skal sørges for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet, kvalitet og tilgjengelighet ved behandling av personopplysninger. For å oppnå en slik tilfredsstillende sikkerhet skal informasjonssystemet og sikkerhetstiltakene dokumenteres (helseregisterloven § 16, personopplysningsloven § 13).

I personopplysningsforskriften [5] og i lovene stilles det krav om at den enkelte virksomhet, ved daglig leder eller tilsvarende, skal etablere et internt styringssystem for informasjonssikkerhet, og ha rutiner for jevnlig sikkerhetsrevisjon (helseregisterloven § 17, person-

opplysningsloven § 14, personopplysningsforskriften § 2-3 og § 2-16). I dette inngår også gjennomføring av risikovurderinger.

Utarbeidelse av bransjevise atferdsnormer er nevnt i lovgivingen (personopplysningsloven § 42 pkt. 6). Helsesektoren var tidlig ute med å få til en slik bransjenorm: ”Norm for informasjonssikkerhet i helsesektoren” [6]. Denne stiller krav som detaljerer og supplerer gjeldende regelverk. Normen er bygd opp med en *styrende* del, en *gjennomførende* del og en *kontrollerende* del. I tilknytning til normen er det utarbeidet et sett med faktaark. Disse beskriver nærmere hvordan enkelte sentrale krav i normen kan oppfylles, og gir praktisk veiledning til dette.

Personopplysningsforskriften § 7-26 påpeker at virksomheter i helsesektoren har meldeplikt til Datatilsynet for all elektronisk behandling av personopplysninger, dvs EPJ-system og elektronisk kommunikasjon. Meldingen skal bekrefte at virksomheten har sikkerhets-dokumentasjon, har utført risikoanalyse og har et opplegg for systemrevisjoner, vedlikehold og versjonskontroll. Se også Datatilsynets egen informasjon om dette [7].

1.2. Om informasjonssikkerhet

Både helseregisterloven [3] og personopplysningsloven [4] definerer informasjonssikkerhet til å omfatte *konfidensialitet*, *integritet* og *tilgjengelighet*; helseregisterloven tar i tillegg med *kvalitet* som et aspekt ved informasjonssikkerhet (helseregisterloven § 16, person-opplysningsloven § 13).

Konfidensialitet:
Sikring av informasjonens konfidensialitet er nært knyttet til taushetsplikten, å hindre at informasjon tilfaller uvedkommende. Personidentifiserbare helseopplysninger er sensitiv informasjon i følge personopplysningsloven (§ 2 pkt. 8). – Uvedkommende er alle de som ikke er i et behandlingsforhold til pasienten.

Av tekniske tiltak som er med på å sikre konfidensialitet kan nevnes kryptering, tilgangs-kontroll (autentisering og autorisering) og logging.

Anonymiserte opplysninger er ikke å regne som sensitiv informasjon.

Integritet:
Sikring av informasjonens integritet innebærer sikring mot utilsiktet eller uautorisert endring av informasjonen. All endring skal kunne spores. Begrepet *ikke-benektning* er nært knyttet til integritet.

Bruk av hash-funksjon og digital signatur er sentrale tiltak for å sikre integritet og ikke-benektning. Tilgangskontroll og logging er viktige mekanismer også i denne sammenheng, samt tiltak mot ødeleggende programvare.

Kvalitet:
Informasjonen skal være fullstendig og korrekt, og ikke misvisende. Dette kan gjerne anses som en del av aspektet integritet – dvs det at informasjon ikke er blitt slettet eller endret. Men særlig når det dreier seg om informasjon i form av bilder, video og lyd har vi sett at kvalitet er et viktig aspekt i seg selv.

Tilgjengelighet:
Sikring av nødvendig tilgang til informasjon, at informasjon skal kunne være tilgjengelig for autorisert personell når de trenger det, henger sammen med kravet om å gi forsvarlig helsehjelp.

Mekanismer for sikring av tilgjengelighet er bl.a. forsvarlig nettforbindelse, backup-rutiner, og sikring mot ondsinnet programvare som kan blokkere tilgang (DoS-angrep).

1.3. Om risikoanalyse

Personopplysningsloven [4] § 31 krever at den databehandlingsansvarlige gir melding til Datatilsynet innen 30 dager før behandling av personopplysninger tar til, eller før det gjøres endringer som får betydning for informasjonssikkerheten. I meldingen skal det bl.a. opplyses om hvilke sikkerhetstiltak som er satt i verk for databehandlingen (§ 32). Det innebærer at det må være gjennomført risikovurdering med hensyn på informasjonssikkerhet før melding kan sendes.

Personopplysningsforskriften [5] § 2-4 ”Risikovurdering” sier at det skal føres oversikt over hva slags personopplysninger som behandles, at virksomheten selv skal fastlegge kriterier for akseptabel risiko forbundet med behandlingen av personopplysninger, og at den behandlingsansvarlige skal gjennomføre risikovurdering for å klarlegge sannsynligheten for og konsekvenser av sikkerhetsbrudd. Resultatet av risikovurderingen skal dokumenteres. Ny risikovurdering skal gjennomføres ved endringer som har betydning for informasjons-sikkerheten.

Det finnes flere veiledninger til gjennomføring av risikovurderinger. Her kan nevnes veiledninger laget av NST [8], av Datatilsynet [9] og av KITH [10].
Risikoanalyseprosessen kan deles inn i fem faser:

1. Identifisere det som skal analyseres – system, tjeneste, omgivelser, bruk
2. Identifisere trusler og uønskede hendelser
3. Validere trusler mhp *konsekvens* og *sannsynlighet*
4. Analysere *risikonivå*
5. Foreslå tiltak som reduserer risikonivå

I det følgende gis en beskrivelse av hver av de fem fasene i gjennomføringa.

Fase 1: Kontekstidentifisering
Til denne fasen hører forarbeid i form av å bestemme hvem som skal delta i prosessen, tidsfrister og ressurser. En plan for prosessen må foreligge.
Det må også lages en beskrivelse av systemet eller tjenesten som skal analyseres, omgivelsene det inngår i og brukere og andre interessenter til systemet. Dersom det som skal analyseres er en del av et større system, må avgrensninger beskrives. En slik system-beskrivelse må formidles til alle deltakere i prosessen for å sikre seg at alle møter med et minimum av entydig/felles kunnskap.
I denne fasen skal deltakerne bli enig om *akseptkriterier* og definere/beskrive verdier for *konsekvens*, *sannsynlighet* og *risikonivå*. Av erfaring kan dette være vanskelig å gjøre så tidlig i analyseprosessen, særlig ved en første gjennomgang av et system, og man må ofte gå tilbake og revurdere dette underveis i prosessen.

Akseptkriteriene skal si noe om uønskede hendelser og om hvor stor/liten risiko vi godtar for slike hendelser, f.eks:

Det er ikke akseptabelt at:

- Pasient får varig skade som en følge av at denne tjenesten ble brukt. (Her bør man i tillegg angi hvor mange slike hendelser som evt. kan "godtas" over en viss tid.)
- Uvedkommende får innsyn i (ser og hører) helseinformasjonen som overføres. (Her bør man i tillegg angi hvor ofte man evt. kan "godta" at dette skjer.)
- Uvedkommende kan endre helseinformasjon under overføring. (Som foran: Angi hva man evt. kan "godta".)

Vi velger å bruke kvalitative betegnelser på konsekvens, sannsynlighet og risikonivå. Eksempler på verdier for disse er vist under fasene 3 og 4 nedenfor.

Fase 2: Trusselidentifisering

Det finnes flere metoder for å komme fram til trusler, sårbarheter, uønskede hendelser – litt avhengig av hvor detaljert spesifikasjon man har av det systemet som skal analyseres. Vi gjennomfører imidlertid ofte denne fasen som en "strukturert brainstorming" – strukturert i den betydning at man til en viss grad leder diskusjonen gjennom bruk av stikkord/ledeord, som f.eks.:

- (Trusler mot informasjonens) Konfidensialitet – Kvalitet – Integritet – Tilgjengelighet
- (Trusler som kommer) Innenfra – Utenfra – "Ovenfra"
- (Hendelser som kan skje) Med overlegg – Uforvarende

Dersom det er vanskelig å komme i gang kan man spørre deltakerne etter "worst case" – hva er det verste som kan skje ved bruk av det aktuelle systemet?
Det som kommer fram i en slik "brainstorming" oppsummeres i en trusseltabell. Tabell 1 viser eksempel på en slik tabell. Her skriver man fortløpende ned trusler / uønska hendelser og deres årsak etter hvert som de foreslås. I tillegg skriver man ned evt. kommentarer som måtte komme, om f.eks. konsekvens og sannsynlighet (men verdier for disse settes ikke i denne omgang).

Tabell 1: Trusseltabell (eksempel)

ID	Trussel	Årsak	Konsekvens	Sannsynlighet	Risiko	**Kommentarer** (f.eks forslag til tiltak)

Som etterarbeid kan man rydde/strukturere tabellen bl.a. ved å skrive ut stikkord, gruppere trusler, slå sammen trusler eller stryke trusler som gjentas. I tillegg gis hver enkelt trussel sin unike id.

Fase 3: Validering av truslenes konsekvens og sannsynlighet

I denne fasen gjennomgår man alle de identifiserte truslene og uønska hendelsene og setter verdier for konsekvens og sannsynlighet på hver av dem.

For hver risikoanalyse må man bli enig om passende verdier og beskrivelser av disse (se fase 1). Antallet verdier man skal bruke for hhv konsekvens og sannsynlighet bestemmer man også. Det vanlige er å bruke 3-5 ulike verdier for hver, og man trenger ikke å ha samme antall verdier for konsekvens og sannsynlighet.

Konsekvens

Tabell 2 viser eksempel på kvalitative verdier for konsekvens, definert utfra ulike kriterier. I dette eksemplet har man brukt fire[1] ulike verdier for konsekvens: Liten – Moderat – Alvorlig – Katastrofal.

[1] Nivået "Ingen" er bare tatt med som eksempel, det blir ikke brukt i den virkelige analysen. (Hvis en trussel ikke har noen konsekvens eller innebærer den ingen risiko.)

Tabell 2: Verdier for konsekvens (eksempel)

Konsekvens	For virksomheten/tjenesten			For person/pasient		
	Lov	**Økonomi**	**Anseelse**	**Liv/helse**	**Økonomi**	**Anseelse, rykte**
Ingen (K=0)	Ingen brudd	Null tap	Null tap	Ingen konsekvens	Null tap	Null tap
Liten (K=1)	Forseelse som ikke fører til reaksjon	Minimalt økonomisk tap som kan gjen-opprettes	Noe tap av anseelse, på kort sikt	Ingen innvirkning på helse	Et lite økonomisk tap som kan gjen-opprettes	Noe tap av anseelse på kort sikt.
Moderat (K=2)	Mindre alvorlig lovbrudd/ forseelse, advarsel/ eller påbud (som første reaksjon)	Økonomisk tap, kan gjen-opprettes	Tap av anseelse, påvirker tillitt og respekt	Ingen umiddelbar innvirkning på helse, eller en liten, forbi-gående virkning på helse	Økonomisk tap, kan gjen-opprettes	Tap av anseelse, kompromit-tering av opplysninger av mindre alvorlig type (f.eks blodtrykks-verdier)
Alvorlig (K=3)	Alvorlig lovbrudd, mindre straff/bøter	Stort økonomisk tap, uopprettelig	Alvorlig tap av anseelse, lengre virkning på tillitt og respekt	Redusert helse	Betydelig økonomisk tap, uopprettelig	Alvorlig tap av anseelse, kompromit-tering av sensitive og krenkende opplysninger
Katastrofal (K=4)	Alvorlig lovbrudd, straff/bøter	Betydelig, økonomisk tap, uopprettelig	Alvorlig tap av anseelse, ødeleggende for tillitt og respekt	Død eller varig ødeleggelse av helse	Betydelig, uopprettelig økonomisk tap	Alvorlig tap av anseelse som varig påvirker liv, helse, økonomi

Sannsynlighet

Tabell 3 viser eksempel på kvalitative verdier for sannsynlighet, definert utfra kriterier som frekvens, letthet, motivasjon. Mest som eksempel er det tatt med en kolonne som viser kvantitative mål for sannsynlighet. Det er imidlertid vanskelig å sette sannsynlighet utfra kvantitative verdier. Da må man ta utgangspunkt i erfaringer, statistikk og historiske data for bruk av et tilsvarende system.

I dette eksemplet er det brukt fire[2] ulike verdier for sannsynlighet: Liten – Middels – Stor – Svært stor.

[2] Nivået "Ingen" er bare tatt med som eksempel, det blir ikke brukt i den virkelige analysen. (Hvis en trussel ikke har noen sannsynlighet innebærer den ingen risiko.)

Tabell 3: Verdier for sannsynlighet (eksempel)

Sannsynlighet	**Frekvens**	**Letthet/Vanskelighetsgrad Motivasjon**	**(kvantitativt)**
Ingen (S=0)	Aldri	Umulig.	0
Liten (S=1)	Hver 50. oppkopling/ bruk eller sjeldnere (>=50)	Må ha detaljkunnskap om systemet. Trenger spesielle hjelpemidler. Kan bare skje med overlegg, bevisst.	< 0,02 < 2 %
Middels (S=2)	Oftere enn hver 50. men sjeldnere enn hver 10. oppkopling/bruk (>=10 og <50)	Normal kjennskap til systemet. Vanlige hjelpemidler. Med overlegg, bevisst.	0,02 – 0,1 2 – 10 %
Stor (S=3)	Oftere enn hver 10. oppkopling/bruk (>=2 og <10)	Kan skje med liten kjennskap til systemet. Uten hjelpemidler. Ved uaktsomhet eller feil bruk. Med overlegg hvis noen er villig til å betale for informasjonen.	0,1 – 0,5 10 – 50 %
Svært stor (S=4)	Annenhver eller hver oppkopling/bruk (<2)	Kan skje uten kjennskap til systemet. Uten hjelpemidler. Ved uaktsomhet eller feil bruk. Med overlegg hvis noen er villig til å betale for informasjonen.	0,5 – 1,0 > 50 %

Fase 4: Analyse av risikonivå

Risiko er produktet av konsekvens og sannsynlighet. Det kan illustreres gjennom ei toveis matrise.

Risikonivået som man har definert i fase 1 kan f.eks. være slik som vist i matrisa i tabell 4. Her har man valgt tre[3] nivå: Lavt – Moderat – Høyt.

[3] Nivået Null er her bare tatt med som eksempel, det utelates i den virkelige analysen.

Tabell 4: Risikomatrise med definisjon av risikonivå (eksempel)

Kons. / **Sanns.**	**Ingen** (K=0)	**Liten** (K=1)	**Moderat** (K=2)	**Alvorlig** (K=3)	**Katastrofal** (K=4)
Ingen (S=0)	Null	Null	Null	Null	Null
Liten (S=1)	Null	Lav 1	Lav 2	Middels 3	Middels 4
Middels (S=2)	Null	Lav 2	Middels 4	Middels 6	Høy 8
Stor (S=3)	Null	Middels 3	Middels 6	Høy 9	Høy 12
Svært stor (S=4)	Null	Middels 4	Høy 8	Høy 12	Høy 16

I fase 1 må man beskrive hva man legger i de ulike nivåene og hvor grensene mellom nivåene skal gå. Det kan f.eks være slik:

Lav (1-2) Akseptabel risiko. Tjenesten kan benyttes med de identifiserte truslene, men man må observere truslene for evt. å oppdage endringer som kan gi økning i risikonivå.

Middels (3-6) Kan være en akseptabel risiko, men i hvert tilfelle må utviklingen av risikoen overvåkes nøye og det må vurderes om risikoreduserende tiltak enkelt kan iverksettes.

Høy (7-16) Uakseptabel risiko. Tjenesten kan ikke tas i bruk før risikoreduserende tiltak er iverksatt.

Ved å plassere alle truslene (med deres unike id) inn i matrisa i forhold til de verdiene de er gitt for konsekvens og sannsynlighet, vil man finne truslenes risikonivå.

Fase 5: Forslag til tiltak
I utgangspunktet må man finne tiltak mot de truslene som har uakseptabel høy risiko. Men det er flere måter å håndtere en risiko på. Man kan:

1. Unngå risikoen – dvs. ikke utsette seg for risikoen, f.eks. ved å ikke gjennomføre det som kan føre til den uønska hendelsen.
2. Redusere risikoen – ved å redusere sannsynlighet og/eller konsekvens. Det er som oftest enklere å redusere sannsynlighet enn konsekvens.
3. Overføre risikoen (f.eks. ved å tegne en forsikring overføres risikoen til et forsikrings-selskap)
4. Akseptere risikoen – leve med den, beholde den. Her er det viktig å merke seg at det å akseptere risikoen betyr ikke at man aksepterer den uønska hendelsen, sikkerhetsbruddet.

Man kan velge en av disse måtene, eller man kan kombinere to eller flere. Risikoreduserende tiltak må vurderes opp mot kost/nytte for tjenesten. Noen tiltak kan redusere risikonivået for flere trusler samtidig, og enkle og billige tiltak som kan redusere en akseptabel risiko bør gjerne iverksettes.

Deretter blir det opp til de ansvarlige for prosjektet/tjenesten å gjennomføre tiltakene: prioritere, sette tidsfrister, utpeke ansvarlige personer, og følge opp arbeidet.

1.4. Trusler, risiko og mulige tiltak

Før risikoanalysen må det foreligge en systembeskrivelse som omfatter teknologien i systemet, tilkopling mot nett (helsenett, internett og evt andre nett), brannmurer og andre sikkerhetstiltak[4]. I tillegg må det være en funksjonell beskrivelse av systemet/tjenesten: Hvilke typer data skal det inneholde (lagre, formidle), hvem er brukerne, til hvilke formål og i hvilke situasjoner skal dette brukes. (Se ellers beskrivelse av Fase 1 foran.)

Basert på det som så langt er kjent om systemet/tjenesten, kan man likevel tenke seg noen mulige trusler eller uønska hendelser. Uten en mer detaljert kjennskap til systemer og uten deltakelse av sentrale personer i prosjektet, er det imidlertid vanskelig å si noe om konsekvens, sannsynlighet og risikonivå for disse truslene. I beste fall kan det som sies i dette avsnittet være utgangspunkt for en grundigere risikoanalyse i et hovedprosjekt.

I vurderingen av mulige trusler kan man inkludere følgende:

1. Konfidensialitet. Kan uvedkommende få tilgang til sensitiv informasjon om pasient? (Men hvor stor er motivasjonen for å få tak slik informasjon?)
    - Informasjon under overføring, på nettet. Er koplingen mot Internett sikker nok? Også innenfor Helsenettet er det mange som ikke skal ha tilgang til denne informasjonen. Informasjon som overføres bør være kryptert, evt at den overføres over en kryptert forbindelse.
    - Ved at de logger seg inn, gir seg ut får å være autorisert bruker. Sikkerheten omkring brukernavn og passord – mange trusler, f.eks ”Social engineering”, Phishing, etc.

[4] Detaljnivået i disse beskrivelsene avhenger av hvor tidlig i utviklingen risikoanalysen gjøres.

- Kan man få til rollebasert tilgang – for alle skal ikke se/gjøre alt. Og sikrere autentisering?
- Er det mulig å få tilgang rett inn til web-basert informasjon gjennom å kopiere en URL, og slik unngå innloggingsprosedyren?
- Hvor lett er det for uvedkommende å se over skuldrene på, se gjennom vindu, åpen dør,…?
- Dersom VK: Hvem andre er til stede på den andre siden, som du ikke ser?
- Hvor sikker er den lokale PC-en? Blir all informasjon sletta fra PC ved utlogging?
- Jobber man hjemmefra, hjemmekontor? Hvordan er tilknytningen til sikkert nett? Har man kontroll på hvem som bruker PC-en? Er det en bærbar som man tar med fra jobb, som ungene bruker til spill og nedlasting,…?
- Hvordan er tilgangen til det som er lagra i databaser, og tilgangen til logg-informasjon? Ligger det sensitiv informasjon i loggene? Hvor mye logges – hele diskusjonen f.eks eller bare at den har funnet sted og når.

2. Kvalitet.
   - Er bilder og evt. video gode nok, tydelige nok, til at man kan gi riktig råd? Her er opplæring og bevisstgjøring viktige tiltak: Være kritisk til det man ser av bilder.
   - Brukergrensesnitt må være så entydige ta de ikke kan lede til misforståelser.

3. Integritet:
   - Kan noen logge seg inn og gi falske råd – gi seg ut for å være en annen?
   - Hvor lett er det å ødelegge databaser og logger? Utilsiktet og/eller med hensikt?
   - Er det lett å gjøre feil som fører til utilsiktet endring/sletting av informasjon som allerede er publisert eller informasjon som ligger i database, logg?
   - Hvilke tiltak er iverksatt? Beskyttelse mot skadelig programvare og rutiner for oppdatering? Autentisering og ikke-benektning?

4. Tilgjengelighet:
   - DoS-angrep?
   - Uforutsette hendelser som kan hindre tilgang?
   - Kan hackere komme inn og ødelegge webstedet? Ødelegge databaser?
   - Backuprutiner. Beskyttelse mot diskcrash.

Annet:

- Åpen e-post, pratekanal (chat), diskusjonsgrupper er alle utsatt for trusler. NHN tilbyr derfor e-post og internett-tilgang via terminalserverløsning. Er dette en adekvat løsning for brukerne, eller vil det føre til at de selv ”ordner seg” med direkte internett-tilgang fra PC-en?
- Det må foreligge avtaler om drift (mellom databehandlingsansvarlig og databehandler), der taushetsplikt er et viktig tema.

- Det åpne web-stedet: Rutiner omkring utlegging av informasjon her. Skal noen ha redaktøransvar? Hva innebærer i så fall dette ansvaret? Er det enkelt å gjøre feil, f.eks uforvarende legge ut sensitiv informasjon der? Eller legge ut på feil sted, dvs der i stedet for det lukka nettet?

Tilsvarende tjenester er utviklet og tatt i bruk og sikkerhetsutfordringene bør derfor være overkommelige.

At de tekniske sikkerhetstiltakene er så gode som mulig er selvsagt viktig, men enda viktigere er det at brukerne får informasjon og opplæring og er bevisst på sitt ansvar.