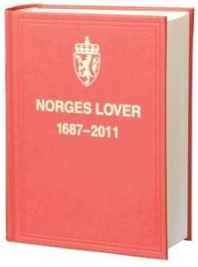
Prosjektrapport

Nye telemedisinske tjenester til hjemmedialysepasienter

Juridiske og sikkerhetsmessige problemstillinger



Eli Arild

Ellen K. Christiansen

Eva Henriksen

Tittel:	**Juridiske og sikkerhetsmessige problemstillinger ved "Nye telemedisinske tjenester til hjemmedialysepasienter"**
NST-rapport:	nr. 03-2013
Prosjektleder:	Eli Arild
Forfattere:	Eli Arild, Ellen K. Christiansen, Eva Henriksen
ISBN:	978-82-8242-034-1
Dato:	2013-01-17
Antall sider:	44
Emneord:	Hjemmedialyse, videokonferanse, ansvar, forsvarlighet, samtykke, taushetsplikt, informasjonssikkerhet, risikovurdering
Oppsummering:	Som en del av EU-prosjektet "Implementing Transnational Telemedicine Solutions" (ITTS), er det installert utstyr for videokonferanse hos to pasienter som utfører peritonealdialyse (PD) hjemme. Tidligere kartlegginger og forprosjekt har ikke gått i dybden på relevante juridiske og sikkerhetsmessige problemstillinger. Det er nå gjort i dette delprosjektet, som er finansiert av "UNN-millionen" i 2012. I tillegg til den juridiske gjennomgangen er det gjennomført en risikovurdering av informasjonssikkerheten i tjenesten, og det er utarbeidet en kortfattet sjekkliste eller veileder med punkter som skal hjelpe til i etableringen av en sikker VK-tjeneste for hjemmedialysepasienter.
Utgiver:	Nasjonalt Senter for samhandling og telemedisin Universitetssykehuset Nord-Norge Postboks 35 9038 Tromsø Telefon: 07766 E-post: info@telemed.no Internett: www.telemed.no

English Summary

Title:

Legal and security issues for "New telemedicine services for home dialysis patients"

Abstract:

As part of the EU project "Implementing Transnational Telemedicine Solutions" (ITT), video-conferencing equipment has been installed with two patients performing peritoneal dialysis (PD) at home. In previous surveys and pilot projects we have not looked deeply into relevant legal and security issues. This has been done in the current project, which is funded by University Hospital of Norh Norway in 2012.

In addition to a review of legal aspects and carrying out a risk assessment of the information security of this service, the work has resulted in guidelines for a secure video conferencing service for home dialysis patients.

Sammendrag

Som en del av EU-prosjektet ”Implementing Transnational Telemedicine Solutions” (ITTS), er det installert utstyr for videokonferanse hos to pasienter som utfører peritonealdialyse (PD) hjemme.

I tidligere kartlegginger og forprosjekt har vi ikke gått i dybden på relevante juridiske og sikkerhets-messige problemstillinger. Det gjøres nå i dette delprosjektet, som er finansiert av Universitetssykehuset Nord-Norge HF i 2012.

Kapittel 2 tar for seg noen sentrale juridiske aspekter som bør diskuteres når hjemmedialyse med oppfølging via videokonferanse ytes fra spesialisthelsetjenesten til pasienter i hjemmet, eventuelt med medhjelpere fra kommunal helsetjeneste.

Overordnet dreier det seg om forhold som kan påvirke forsvarligheten av tjenesten. Vi har diskutert temaer knyttet til ivaretakelse av pasientens rett til privatlivets fred. Vi har også diskutert enkelte særlige forhold knyttet til helsepersonellets ivaretakelse av taushetsplikten ved bruk av videokonferanse. Pasientens rett til personvern og ansvar og ansvarsforhold er også tatt opp. Avslutningsvis foreligger noen betraktninger om pasientens samtykke som grunnlag for tjenesten.

I kapittel 3 presenteres grunnleggende krav til informasjonssikkerhet. Det er gjennomført en risiko-vurdering av tjenesten mht. informasjonssikkerhet. En oppsummering av risikovurderingen er tatt med i kapittel 3.

I risikovurderingen ble det identifisert nærmere 40 mulige trusler mot sikkerhetsaspektene konfidensialitet, kvalitet, integritet og tilgjengelighet. Truslene ble analysert med hensyn til konsekvens og sannsynlighet. Det samlede risikobildet viser at ingen trusler er vurdert til å ha *høy* risiko, og ingen trusler anses å ha katastrofal konsekvens. 7 trusler har *middels* risiko, mens de resterende 30 er vurdert å ha *lav* risiko. Dette er en god indikasjon på at det overordna risikonivået kan anses å være lavt i VK-tjenesten for hjemmedialyse. Det lave risikonivået er også et resultat av de tiltak som allerede er gjort for å oppnå tilfredsstillende sikkerhet. Alle truslene er analysert til å ha *akseptabel* risiko.

Det er likevel en rekke enkle tiltak som kan og bør gjennomføres for å holde risikoen på et lavest mulig nivå. Blant tiltakene finnes både praktiske, organisatoriske tiltak, og tiltak som allerede er lagt inn i tjenesten. Rapporten har foreslått tiltak under kategoriene prosedyrer og rutiner, opplæring, fysiske tiltak og konfigurering av utstyr.

En full rapport fra risikovurderingen finnes som vedlegg B og C i denne rapporten.

Ett av målene ved dette delprosjektet var å lage en kortfattet sjekkliste eller veileder med punkter som skal hjelpe til i etableringen av en sikker VK-tjeneste for hjemmedialysepasienter. En slik sjekkliste er tatt med som vedlegg A.

UNN v/ Medisinsk klinikk v /leder har vært prosjekteier.

Prosjektgruppen har bestått av:

- Eli Arild, prosjektleder ved NST
- Ellen Kari Christiansen, juridisk seniorrådgiver, NST
- Eva Henriksen, sikkerhetsrådgiver, NST

Prosjektet ble gjennomført i perioden august til desember 2012.

Innhold

1 Innledning 9
1.1 Bakgrunn 9
1.2 Om hjemmedialyse 9
1.3 Telemedisinske tjenester til hjemmedialysepasienter 10
1.4 Om dette delprosjektet 11

2 Juridiske betraktninger 12
2.1 Kravet til forsvarlig virksomhet 12
2.2 Privatlivets fred og taushetsplikten 13
2.2.1 Privatlivets fred 13
2.2.2 Ivaretakelse av taushetsplikten 13
2.2.3 Frykt for «hacking» 13
2.3 Ansvar og ansvarsforhold 13
2.3.1 Regelverket 13
2.3.2 Helsevesenets ansvar 14
2.3.3 Pasientens og pårørendes ansvar 15
2.3.4 Ansvarsfordeling mellom sykehus og kommunalt helsepersonell 15
2.4 Pasientens samtykke. Grunnlaget for tjenesten 16
2.5 Oppsummerende punkter 16

3 Informasjonssikkerhet og risikovurdering 17
3.1 Krav til informasjonssikkerhet 17
3.2 Risikovurdering 18
3.2.1 Metode 18
3.2.2 Resultater 19

4 Oppsummering 21

Referanser 22

Vedlegg A Videokonferansestøtte for hjemmedialyse. Sjekkliste (veileder) 23
A1 Sjekkliste for sykehusets helsepersonell 23
A2 Sjekkliste for pasientsiden av konferansen 26

Vedlegg B Rapport fra risikovurdering 29
B.1 Metode og gjennomføring 29
B.2 Definisjoner av konsekvens, sannsynlighet og risiko 30
B.2.1 Konsekvens 30
B.2.2 Sannsynlighet 30
B.2.3 Risiko 31
B.2.4 Akseptkriterier 32

B.3 Trusselkartlegging og analyse 32
B.3.1 Trusler mot konfidensialitet 33
B.3.2 Trusler mot kvalitet 35
B.3.3 Trusler mot integritet 36
B.3.4 Trusler mot tilgjengelighet 36
B.4 Forslag til tiltak 36

Vedlegg C Trusseltabellen 38

1 Innledning

1.1 Bakgrunn

Høsten 2008 ble forprosjektet "Kartlegge behov for nye telemedisinske løsninger hjem til nyresvikt-pasienter" gjennomført[1] [1]. I følge forprosjektrapporten mente pasienter med dialysemaskiner i hjemmet at telemedisinske løsninger kunne bidra til nær kontakt med og oppfølging fra sykehuset. I dag bruker hjemmedialysepasientene telefon i kontakten med sykehuset. Det er imidlertid en utbredt oppfatning at bruk av videokonferanse (VK) vil være nyttig i problemløsningssituasjoner, både hjem til pasienten og til for eksempel sykehjem [2].

I perioden september 2011 til februar 2012 ble prosjektet "Nye telemedisinske tjenester til hjemme-dialysepasienter" gjennomført[2]. Prosjektet skulle installere videokonferanse hjemme hos en PD-pasient og en HHD-pasient. Det viste seg at det ikke var mulig å rekruttere en HHD-pasient i løpet av prosjektperioden. PD-pasienten ble akutt syk og døde dessverre, og vi kom aldri i gang med å bruke videokonferanseutstyret som var installert i pasientens hjem. Arbeidet i prosjektet ble dokumentert i en egen rapport [3].

Prosjektet blir videreført i et pågående EU-prosjekt: "Implementing Transnational Telemedicine Solutions" (ITTS) [4] som vil bli avsluttet desember 2013. Målet er å implementere videokonferanse i hjemmet til to PD-pasienter og en HD-pasient. To PD-pasienter fikk utstyr hjem i juni 2012 og begge bruker utstyret jevnlig i kontakten med Nyreavdelingen på UNN.

Bakgrunnen for *dette* delprosjektet er at vi tidligere ikke har gått i dybden på relevante juridiske og sikkerhetsmessige problemstillinger. I den forrige rapporten [3] pekte vi på en del forhold som burde drøftes nærmere, da vi anser dette som en forutsetning for å kunne etablere gode og bærekraftige løsninger på sikt.

1.2 Om hjemmedialyse

I det følgende gis en kort beskrivelse av de ulike formene for dialyse i hjemmet.

Peritonealdialyse i hjemmet (PD)

PD blir utført av pasienten selv hjemme eller i en kommunal institusjon. Ved assistert PD gis assistanse av opplært personell fra kommunehelsetjenesten. Behandlingen kan utføres på to måter:

1. Ved manuelle poseskift (CAPD), som er den meste benyttede metode, brukes tyngdekraften til å tømme ut brukt væske fra bukhulen og erstatte denne med ny væske. Dette gjøres på dagtid med poseskift 3-5 ganger i døgnet.
2. Ved automatisk peritonealdialyse (APD) brukes en maskin for å utføre poseskiftene om natten mens pasienten sover.

Hemodialyse i hjemmet (HHD)

Ved HHD kobler pasienten seg til og fra HD-maskinen selv og overtar i høy grad den funksjonen HD-sykepleieren på sykehuset ellers har. Denne behandlingen krever mye av pasienten, og forutsetter at det brukes ressurser på opplæring og installasjon av utstyr i pasientens hjem. HHD kan også utføres med assistanse av spesialtrenet sykepleier fra kommunehelsetjenesten.

HHD har så langt ikke hatt særlig utbredelse i Norge. Dette henger sammen med den høye transplantasjonsraten i Norge, samt utbredelsen av peritoneal dialyse som en velegnet metode for bruk i hjemmet. HHD krever ferdigheter hos pasienten, både med hensyn til det tekniske utstyret og oppsettet av maskinen, men det som kanskje er mest krevende er stikking i fistel og tilkobling av blodtilgangen til maskinen. Ved UNN tar opplæringen av pasienten rundt tre måneder. Det er pasienter som er stabile i hemodialyse som kan benytte seg av dette.

[1] Finansiert av InnoMed
[2] Finansiert av UNN

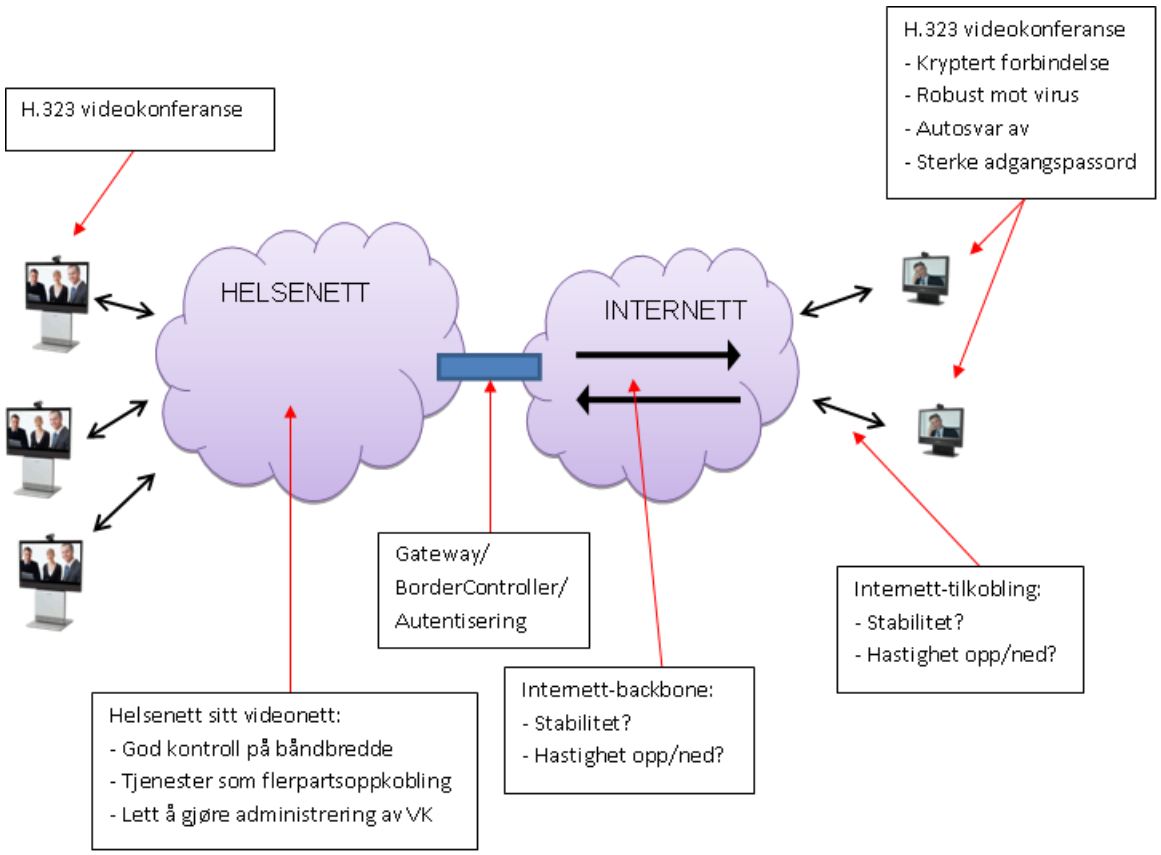
På grunn av muligheter for å kunne få hyppigere og lengre dialyse, gir HHD ofte både medisinske og psykososiale forbedringer. Pasientene opplever bedre allmenntilstand, frihet og mulighet til å jobbe. Livskvaliteten øker og pasientene kan ofte leve et nesten normalt liv: mindre kostrestriksjoner, et normalt væskeinntak, redusert medikamentbehov, normalisering av blodtrykk, kognitive funksjoner, bedre søvn og ernæringstilstand, samt færre sykehusinnleggelser

1.3 Telemedisinske tjenester til hjemmedialysepasienter

Som en del av EU-prosjektet "Implementing Transnational Telemedicine Solutions" (ITTS), er det installert utstyr for videokonferanse hos to pasienter som utfører peritonealdialyse (PD) hjemme. De fikk videokonferanseutstyr hjem i juni 2012, og begge bruker dette til å kommunisere med sykepleier på Nyremedisinsk avdeling på UNN.

Figur 1 viser hvordan VK-utstyret er plassert i nettet. Videokonferanseenheten på avdelingen på UNN står på videonettet i Norsk Helsenett. Hjemme hos pasientene er VK-enheten fysisk tilkoplet Internett. Enheten er dermed synlig for andre enheter på Internett. Disse enhetene er imidlertid også registrert som enheter i "Gateway" hos Norsk Helsenett og er således logisk sett VK-enheter tilknyttet helsenettet. Det gjør det mulig for disse enhetene å ringe inn til VK-enheter i helsenettet. (Normalt skal man ikke kunne ringe inn fra et eksternt nett *til* helsenettet, bare internt *i* helsenettet eller ut *fra* helsenettet til et åpent nett som f.eks. Internett.)

Tilkoplingen til Internett kan være forskjellig hjemme hos de ulike pasientene, avhengig av tilbud fra lokal nettleverandør. Dette kan påvirke kvaliteten til nettforbindelsen. I noen tilfeller kan det være stabile nett via fiberkabel, i andre tilfeller kan det være løsninger via gamle kopperkabler eller via radiolink. (I dette prosjektet er den ene pasienten tilknyttet Internett via fiber, mens den andre pasienten ikke har mulighet for slik tilkopling.)



Figur 1: Skisse av videokonferanseløsningen plassert i nettet

I denne tjenesten for hjemmedialysepasienter kan helsepersonell på sykehuset og pasient hjemme kommunisere med hverandre til avtalte tidspunkt. Videokonferansen kan initieres enten fra sykehuset

eller fra pasienten. I begge tilfeller ringer man opp et nummer som er forhåndslagret på enheten. Fra VK-enheten på sykehuset kan helsepersonellet fjernstyre kamera hos pasienten (zoom, posisjon).

Ved å bruke tjenester i helsenettet kan man sette opp flerpartskonferanser, og pasientene hjemme kan delta i slike flerpartskonferanser. I dette prosjektet vil det imidlertid bare være konferanse med en pasient om gangen.

Enhetene på begge sider har "autosvar" slått av, dvs. at videokonferansen ikke koples opp før den andre parten manuelt aksepterer oppringingen ("tar av røret").

Det er mulig å logge seg inn på enhetene via nettet. Dette gjøres normalt av vedlikeholdsmessige grunner. For å unngå at uvedkommende gjør slik fjerninnlogging via nettet, er det lagt inn svært sterke passord på enhetene.

Det er lagt inn obligatorisk ende-til-ende kryptering av videokonferanseforbindelsen[3]. Det innebærer at dersom den ene parten ikke er i stand til å gjennomføre slik kryptering, vil forbindelsen ikke bli etablert.

1.4 Om dette delprosjektet

I dette delprosjektet ønsker vi å legge til rette for bruk av hjemmedialyse med videokonferansestøtte i fremtiden ved å peke på og drøfte på hvilken måte juridiske og sikkerhetsmessige implikasjoner kan ivaretas til beste for pasientene.

Formål

Formålet med delprosjektet er å legge til rette for at både involvert helsepersonell og pasienter kan føle seg trygge på at de juridiske og sikkerhetsmessige forhold rundt tjenesten er ivaretatt, og at samhandlingen rundt tjenesten derved blir god.

Hovedmål

Hovedmålet med delprosjektet er å sørge for at de nødvendige juridiske og sikkerhetsmessige implikasjoner blir klarlagt når videokonferansestøtte ved hjemmedialyse benyttes, slik at pasientens rettsikkerhet og rettigheter i henholdt til helselovgivningen ivaretas når de velger denne behandlingen.

Delmål

1. Gjennomgang og utredning av relevante juridiske problemstillinger, bygd på det arbeidet som ble påbegynt i forbindelse med prosjektet "Nye telemedisinske tjenester til hjemmedialysepasienter"
2. Gjennomføre risikovurdering av informasjonens konfidensialitet, integritet, kvalitet og tilgjengelighet (dvs. i forhold til helseregisterloven og personopplysningsloven med forskrift)
3. Utarbeidelse av en veiledning/sjekkliste knyttet til juridiske og sikkerhetsmessige forhold til bruk i etablering og oppfølging av hjemmedialyse med videokonferansestøtte i fremtiden

Finansiering og organisering

Prosjektet er finansiert av "UNN-millionen" fra Universitetssykehuset Nord-Norge. (UNN avsatte i 2012 en million kroner til telemedisinske prosjekt i klinikkene.)

UNN v/ Medisinsk klinikk v /leder har vært prosjekteier.

Prosjektgruppen har bestått av:

- Eli Arild, prosjektleder ved NST
- Ellen Kari Christiansen, juridisk seniorrådgiver, NST
- Eva Henriksen, sikkerhetsrådgiver, NST

Prosjektet ble gjennomført i perioden august til desember 2012.

[3] 128 bits AES-kryptering

2 Juridiske betraktninger

2.1 Kravet til forsvarlig virksomhet

Kravet om å drive forsvarlig virksomhet (ansvarlig praksis) i helsevesenet gjelder både på individnivå og på virksomhetsnivå. Forsvarlighetskravet er en rettslig og faglig norm eller standard. Dette innebærer at kravene vil endres over tid, i takt med endring i kunnskaper og muligheter, og i forhold til helsepersonellets kompetanse og den situasjonen som skal vurderes. Hva som ligger i kravet til forsvarlighet vil til enhver tid blant annet påvirkes av faglige normer og muligheter, tilsyns-myndighetene og domstolene.

Helsepersonelloven § 4 stiller opp et krav om at

> ”Helsepersonell skal utføre sitt arbeid i samsvar med de krav til faglig forsvarlighet og omsorgsfull hjelp som kan forventes ut fra helsepersonellets kvalifikasjoner, arbeidets karakter og situasjonen for øvrig.»

Kravet til forsvarlighet i spesialisthelsetjenesten reguleres av spesialisthelsetjenesteloven § 2-2. Den oppstiller et krav om at

> «Helsetjenester som tilbys eller ytes i henhold til denne loven skal være forsvarlige. Spesialisthelsetjenesten skal tilrettelegge sine tjenester slik at personell som utfører tjenestene, blir i stand til å overholde sine lovpålagte plikter, og slik at den enkelte pasient eller bruker gis et helhetlig og koordinert tjenestetilbud.»

Kravet til forsvarlighet er etter dette både et personlig ansvar for det enkelte helsepersonell og et ansvar for eiere og ledere av virksomhetene som skal tilrettelegge sin virksomhet slik at helse-personellet kan oppfylle sine plikter på en forsvarlig måte. I Ot.prp. nr 10 (1998-1999) Om lov om spesialisthelstjenester m m ble det på s 122 fremhevet at alle helsetjenester som var omfattet av loven skulle være forsvarlige når de tilbys eller ytes. Det heter:

«Plikten innebærer også at eier av og ledelsen ved f. eks. et sykehus har et ansvar for å legge forholdene til rette slik at det enkelte helsepersonell kan utføre sine oppgaver på en forsvarlig måte. Eksempler kan være at det medisinsk-tekniske utstyret fungerer og at helsepersonellet er kvalifisert i forhold til den oppgaven de utfører. (…) (min understrekning).

Det siste er spesielt interessant i relasjon til tjenester der bruk av slikt utstyr er en forutsetning for den aktuelle tjeneste.

Spørsmålet om forsvarlighet er berørt i rundskriv I-12/2001 Telemedisin og ansvarsforhold (ansvarsrundskrivet)[4]. Det er der påpekt at helsepersonell ikke skal gå ut over sin kompetanse i forbindelse med helsehjelp til pasienter. Dette innebærer en plikt for hver enkelt til å vurdere hvorvidt han/hun har tilstrekkelig kompetanse til å ivareta de oppgaver som til enhver tid skal ivaretas. Det er i denne forbindelse understreket at helsepersonellet må vurdere om vedkommende har den nødvendige informasjon om pasientens sykdomsforløp, symptomer m.v. til å diagnostisere og iverksette behandling. Det sies også eksplisitt at bruk av telemedisin ikke endrer de ordinære ansvarsforhold.

Om telemedisinske virkemidler heter det i rundskrivet at det ikke er avgjørende hvordan informasjonen om pasienten er mottatt. Det som er avgjørende, er at den mottatte informasjon er av tilstrekkelig kvalitet til at helsepersonellet forsvarlig kan ivareta sine oppgaver. Dette er en vurdering den enkelte må foreta forløpende i kontakten med pasienten.

Kort oppsummering:
Ved bruk av telemedisinske virkemidler gjelder, som ellers, kravet til forsvarlig virksomhet, både på systemnivå og for den enkelte helsearbeider. Ved bruk av elektroniske medier i pasientkontakt må virksomheten sørge for at det tekniske utstyret til enhver tid er i orden. Den enkelte helsearbeider må på sin side vurdere om den informasjonen som mottas har så god kvalitet at den kan danne grunnlaget for ytelse av helsehjelp. I motsatt fall må informasjon innhentes på andre måter.

[4] Rundskriv I-12/2001 Telemedisin og ansvarsforhold (ansvarsrundskrivet), Sosial- og helsedepartementet, 05.02.2001

2.2 Privatlivets fred og taushetsplikten

Hjemmedialyse, slik det har vært praktisert til nå, innebærer at helsetjenester som tidligere ble tilbudt i sykehus, nå tilbys i pasientens hjem. Dette medfører nye utfordringer i seg selv. Bruk av video-konferanse mellom personell på dialyseavdelingen og pasientens hjem for å bedre tilbudet, reiser i tillegg blant annet særlige spørsmål knyttet til både taushetsplikt og retten til privatlivets fred.

2.2.1 Privatlivets fred

Man kan si det slik at dette tilbudet medfører at sykehuset får et «kikkhull» inn i pasientens hjem. Slik bruk har av mange vært trukket frem som en «invasjon» av pasientens private sfære [5]. Utplassering av kamera medfører at mennesker som ikke er fysisk til stede, i dette tilfellet sykehusansatte, gis mulighet til å observere private forhold på en annen måte enn tidligere. Dette medfører behov for å avveie hensynet til privatlivets fred mot nytten av å overvåke pasienten i en gitt situasjon. Det må også innarbeides rutiner som gjør risikoen for mulig krenkelse av privatlivets fred minst mulig

2.2.2 Ivaretakelse av taushetsplikten

Datatilsynet er blant dem som har satt fokus på at ny teknologi i helsevesenet og omsorgssektoren medfører helt nye utfordringer. De har blant annet pekt på at ved det de har kalt “alminnelig dialog” mellom pasient og helsepersonell, ser pasienten hvem de kommuniserer med. Dette er ikke alltid tilfellet (“ikke alltid like klart”) ved elektronisk kommunikasjon [6].

Dette gjelder ikke bare for pasienten, det samme gjelder for helsepersonellet. Dette skaper utfordringer i forhold til taushetsplikten.

Hensynet til taushetsplikten, og derved forsvarlighetskravet, tilsier at det helsepersonell som har kontakt med pasienten via videokonferanse, må skaffe seg kunnskap om hvem som eventuelt hører og ser det som blir sagt og gjort. De må med andre ord ha oversikt over hvem som er til stede sammen med pasienten og som de kanskje ikke ser. Dette gjelder selv om pasienten skulle mene at alt kan sies i nærvær av den eller de som måtte være der. Helsepersonellet har uansett en selvstendig plikt til å vurdere hvilke eventuelle begrensninger taushetsplikten kan tenkes å medfører i situasjonen.

Det må innarbeids rutiner som gjør risikoen for brudd på taushetsplikten minst mulig, jf. sjekklisten i vedlegg A.

2.2.3 Frykt for «hacking»

Frykt for “hacking” ble også trukket frem i rapporten “How Can Telehomecare Support Informal Caregiving? Examining What is Known and Exploring the Potential” [5]. I tillegg til følelsen av eller frykten for å bli overvåket, var det enkelte som også var bekymret for om noen kunne “hacke” seg inn i systemet og tilegne seg opplysninger om pasienten. Dette gjorde en del pasienter og pårørende mindre motiverte for å ta utstyret i bruk.

Det er viktig at disse problemstillingene tas opp med pasienten i forkant av en etablering av tjenesten. Pasienten har krav på å vite hva sykehuset har gjort for å forhindre brudd at opplysninger om pasienten kommer på avveier. Dette må formidles til pasienten i en forståelig form. Tiltakene baseres på resultater fra risikovurdering av informasjonssikkerheten ved tjenesten.

Det må innarbeids rutiner som gjør risikoen for mulig hacking minst mulig, jf. sjekklisten i vedlegg A.

2.3 Ansvar og ansvarsforhold

2.3.1 Regelverket

Når det gjelder ansvarsforhold i forbindelse med tjenester som ytes utenfor de fysiske rammene av helseinstitusjoner i situasjoner der pasient og helsepersonell ikke møtes ansikt-til-ansikt, er det lite eller ingenting å hente i lovgivningen. Helselovgivningen og forarbeidene til den inneholder knapt nok en eneste henvisning til begreper som telemedisin, Internett og eHelse [7].

Det foreligger imidlertid et rundskriv om telemedisin og ansvar fra 2001 («ansvarsrundskrivet») [8]. Rundskrivet gjelder bruk av telemedisin i konsultasjon og diagnostikk, og legger til grunn prinsipper som er svært relevante for hjemmedialyse.

Det slås innledningsvis i rundskrivet fast at ansvarsforholdene knyttet til en medisinsk konsultasjon

> *"ikke er annerledes når telemedisinske virkemidler benyttes, enn når mer innarbeidete behandlingsmåter anvendes".*

Det er også uttalt følgende:

> *"telemedisin er et virkemiddel som ikke rokker ved den grunnleggende lovgivning som gjelder helsetjenesten."*

Det er gitt noen eksempler på spørsmål som rutinemessig bør avklares før en telemedisinsk konsultasjon iverksettes:

- *Hva slags situasjon dreier det seg om; en henvisning fra primærlege til spesialist eller rådgivning fra spesialist til primærlege?*
- *Er informasjonen som er mottatt tilstrekkelig til å foreta en forsvarlig vurdering?*
- *Hvem skal føre journal?*

Det er også understreket at ved bruk av telemedisin bør det avklares på forhånd hvilke forutsetninger som er lagt til grunn. Dette vil blant annet inkludere en avklaring av hvem som har ansvar for hva, som alle er innforstått med. Det er også pekt på at den enkelte virksomhet bør etablere systemer som sikrer at bruk av telemedisinske virkemidler gir pasienten en forsvarlig undersøkelse og/eller behandling.

Prinsipper vedrørende ansvar og ansvarsfordeling må innarbeids i gjeldende rutiner slik at ansvarsfordelingen og det som følger av den er tydeliggjort, jf. sjekklisten i vedlegg A.

2.3.2 Helsevesenets ansvar

I InnoMed-rapporten fra 2009 om behov for nye telemedisinske løsninger hjem til nyresviktpasienter, er spørsmålet om ansvar og ansvarsfordeling berørt i flere sammenhenger [1]. Det er blant annet slått fast at sykehuset har det medisinske ansvaret for hjemmedialysetjenesten. Det er vanskelig å se at dette skulle endres som følge av at det innføres videokonferansestøtte.

Dette harmonerer også godt med det som følger av de prinsipper som ligger til grunn for "ansvars-rundskrivet" [8]: Bruk av telemedisin, i dette tilfelle noe som bidrar til at pasienten ikke må oppsøke helsevesenet for dialyse, men kan motta en trygg og sikker tjeneste hjemme, rokker ikke ved den grunnleggende lovgivningen som gjelder helsetjenesten. Ansvarsforholdene knyttet til en medisinsk konsultasjon endres ikke. Igjen: **Ansvarsfordelingen er ikke annerledes når telemedisinske virkemidler benyttes, enn når mer innarbeidete behandlingsmåter anvendes.**

Ivaretakelsen av dette ansvaret kan imidlertid tenkes å stille andre krav til sykehuset enn når tjenesten ytes innenfor virksomhetens fire vegger.

I lov om spesialisthelsetjenester [9] § 2-3 stilles det krav om at helsetjenester som tilbys eller ytes etter loven skal være forsvarlige. I kommentaren til bestemmelsen [10] er det særlig trukket fram det ansvar eiere og ledere har for å sikre at tjenester som tilbys er i samsvar med den minstestandard som forsvarlighetskravet angir. I den forbindelse heter det:

> *"Eksempler kan være at det medisinsk-tekniske utstyret fungerer og at helsepersonellet er kvalifisert i forhold til den oppgaven de utfører."*

Spesialisthelsetjenestens ansvar vil både være knyttet til det utstyr som benyttes og til opplæring av det personell som skal benytte det. Implisitt i spesialisthelsetjenestens ansvar ligger også spesialist-helsetjenestens ansvar for opplæring av eventuelle pasienten som brukere av utstyret. Dette er ikke omtalt eksplisitt. Det er derimot spesialisthelsetjenestens ansvar for at tjenesten er forsvarlig - i alle ledd.

Når en medisinsk tjeneste plasseres hjemme hos pasienten som et ledd i den helsehjelp sykehuset yter, vil det, som ellers, være sykehusets ansvar å påse at totaliteten i tilbudet er forsvarlig. Dette inkluderer ansvar for en lang rekke forhold, derunder ansvar for at teknikken fungerer. Det kan også være påkrevet å skaffe seg oversikt over frekvensen av strømbrudd i området og legge en

beredskapsplan for slike situasjoner, i og med at nødaggregat ikke er standard i de fleste hjem. Det er videre behov for å se nærmere på hvordan en skal organisere "mottaket" i sykehus slik at det nødvendige helsepersonellet er tilgjengelig når pasienten trenger det. Opplæring i alle ledd er også et tema.

2.3.3 Pasientens og pårørendes ansvar

Pasientenes ansvar er omtalt i InnoMed-rapporten fra 2009 [1], men da kun i forbindelse med hjemmedialyse uten videokonferansestøtte. Pasienten er i den forbindelse blant annet omtalt som "utfører" av behandlingen.

Ved bruk av videokonferanse vil pasienten i tillegg måtte bidra til at denne fungerer etter hensikten. Pårørendes rolle er lite berørt. Det forutsettes imidlertid at i de tilfeller pårørende har en rolle, vil den enten overlappe eller erstatte den rolle pasienten er tiltenkt innenfor tjenesten.

I den samme InnoMed-rapporten har pasientene uttalt seg om betydningen av videokonferanse i forbindelse med dialysebehandlingen. En pasient uttalte at bruk av videokonferanse ville redusere hennes ansvar

> *"fordi det er sykehuset som er ansvarlig for behandlingen, og hun utfører denne på vegne av sykehuset."*

Når pasienter og pårørende utfører konkrete oppgaver som en del av en helsetjeneste spesialist-helsetjenesten har ansvaret for, er det som ellers spesialisthelsetjenestens ansvar at tjenesten er forsvarlig, totalt sett. De må derfor påse at pasienter og pårørende som skal medvirke ved utførelsen av tjenesten, er i stand til å ivareta sine oppgaver på en måte som gjør at tjenesten er forsvarlig. I motsatt fall må helsetjenesten finne andre måter å innrette tilbudet på, for eksempel å innhente assistanse fra andre medhjelpere lokalt.

En tjeneste som dette stiller store krav til dialogen mellom helsevesen og pasient. Det må inngå i rutinebeskrivelsene at pasienten forplikter seg til å benytte og ivareta utstyret slik sykehuset har lagt opp til, at pasienten må melde fra dersom utstyret ikke fungerer som forutsatt og ellers melde fra dersom de føler at de ikke mestrer bruken, jf. sjekklisten i vedlegg A.

2.3.4 Ansvarsfordeling mellom sykehus og kommunalt helsepersonell

En kan også tenke seg at hjemmedialyse med videokonferansestøtte benyttes for pasienter i institusjon eller eget hjem med assistanse fra hjemmetjenesten eller annet helsepersonell. I slike tilfeller tildeles helsepersonellet praktiske oppgaver som bidrar til en forsvarlig tjeneste, totalt sett. Dette omfatter, foruten oppsett og bruk av dialyseutstyret, også riktig bruk av videokonferanseutstyr. Disses oppgaver er i og for seg ikke så ulike de oppgaver pasienten, pårørende eller andre hjelpere har eller kan ha ved hjemmedialyse med videokonferansestøtte.

Ut fra prinsippet om at bruk av telemedisin ikke endrer de ordinære ansvarsforhold, tas det utgangs-punkt i at det medisinske ansvaret for tjenesten også i denne sammenheng er tillagt spesialisthelse-tjenesten.

I slike tilfeller anser vi at det kommunalt ansatte helsepersonell skal defineres som medhjelpere for spesialisthelsetjenesten i henhold til spesialisthelsetjenesteloven § 5 [9]. Spesialisthelsetjenesten har med andre ord det totale ansvaret for forsvarligheten. Det omfatter et definert ansvar for en forhånds-vurdering av medhjelperens kompetanse, opplæring og oppfølging i form av løpende tilsyn og nødvendige instruksjoner fra spesialisthelsetjenestens side overfor de kommunalt ansatte med-hjelpere. Dette omfatter også en plikt for spesialisthelsetjenesten til å være tilgjengelig for råd, veiledning og instruksjon underveis i den grad dette er nødvendig for en forsvarlig tjeneste [11].

Eventuelle medhjelpere vil i tillegg ha et selvstendig ansvar for at den helsehjelp de står for er forsvarlig.

Hvordan dette skal legges opp må avtales mellom de impliserte i tråd med de grunnleggende prinsipper i "ansvarsrundskrivet" [8] og innarbeides i gjeldende rutiner, jf. sjekklisten i vedlegg A.

2.4 Pasientens samtykke. Grunnlaget for tjenesten

Det har vært stilt spørsmål ved om det bør inngås en eksplisitt avtale med pasienten rundt hjemmedialyse der sykehusets plikter, pasientenes rettigheter og partenes roller er beskrevet. Et alternativ til dette kan være at pasienten skriver under på en samtykkeerklæring til at behandlingen skjer i hjemmet med videokonferansestøtte.

Etter vår oppfatning og i tråd med ansvarsrundskrivets grunnleggende prinsipper, ser vi ingen grunn til å innføre særlige ordninger for telemedisinske tjenester i hjemmet på dette området. Når dialysen finner sted i hjemmet med videokonferansestøtte, vil dette bli ansett som en del av sykehusets ordinære tilbud der grunnlaget for behandlingen, som ellers, er pasientens samtykke. I henhold til pasient- og brukerrettighetsloven § 4-2 [12], kan et samtykke gis uttrykkelig eller stilltiende. Dersom det trekkes tilbake i henhold til pasient- og brukerrettighetsloven § 4-1, skal den som yter helsehjelp gi nødvendig informasjon om betydningen av at helsehjelpen ikke gis. Det samme må gjelde dersom tilbaketrekningen medfører at helsehjelp må ytes i andre former eller innenfor andre rammer. Det mest nærliggende alternativet vil være hjemmedialyse uten videokonferansestøtte dersom dette vurderes som forsvarlig. Dialyse på satellitt eller i sykehus med nefrolog representerer andre alternativer for en del pasienter.

I tråd med de vanlige prinsipper for pasientens rett til medvirkning og informasjon, vil under alle omstendigheter pasientene ha krav på informasjon om tilbudet og hvilke tiltak sykehuset har satt i verk for å sikre forsvarligheten av det.

2.5 Oppsummerende punkter

Vi har i det foregående tatt for oss noen sentrale juridiske aspekter som bør diskuteres når hjemmedialyse med oppfølging via videokonferanse ytes fra spesialisthelsetjenesten til pasienter i hjemmet, ev. med medhjelpere fra kommunal helsetjeneste. Enkelte juridiske spørsmål vil også være diskutert i forbindelse med risikoanalysen.

Alle spørsmålene knytter seg til forhold som kan innvirke på forsvarligheten av tjenesten, totalt sett. Vi har vært opptatt av å legge til rette for å ivareta pasientens rett til privatlivets fred. I tillegg har vi diskutert forhold knyttet til helsepersonellets ivaretakelse av taushetsplikten, pasientens rett til personvern og ansvar og ansvarsforhold. Det foreligger også noen betraktninger om samtykke.

Involveringen av kommunalt ansatt helsepersonell i eller utenfor institusjon vil kunne tilrettelegges slik at disse får et formelt medhjelperansvar, jf. spesialisthelsetjenesteloven § 5 [9]. Dette medfører at de skal følges opp fra spesialisthelsetjenestens side, samtidig som de også kan få et rettslig (med-) ansvar dersom noe skulle gå galt.

Når videokonferanse benyttes, stiller det krav til kunnskaper og ferdigheter ut over det som knytter seg til bruk av dialyseutstyret. Som ansvarlig for tjenesten, vil det være opp til spesialisthelsetjenesten å legge til rette for at denne delen av tilbudet blir ivaretatt på en forsvarlig måte.

En konkretisering av mulige rutiner og sjekkpunkter fremgår av den utarbeidete sjekklisten. De viktigste aspektene vil også bli tatt opp i et faktaark utgitt av NST første halvår 2013: Hjemmedialyse med videokonferansestøtte.

3 Informasjonssikkerhet og risikovurdering

I begrepet *informasjonssikkerhet* inkluderer Helseregisterloven (§ 16) [13] aspektene konfidensialitet, kvalitet, integritet og tilgjengelighet.

- Konfidensialitet: Personidentifiserbare helseopplysninger er *sensitiv* informasjon (Personopplysningsloven § 2) [14]. Kravet om taushetsplikt i Helsepersonelloven (§ 21) [15] innebærer at slik informasjon ikke skal tilfalle uvedkommende. Uvedkommende er alle som ikke er i et behandlingsforhold til pasienten.
- Kvalitet: Informasjonen skal være riktig, ikke misvisende. Innføring av en teknisk/elektronisk løsning skal ikke bidra til at informasjonen kan misforstås.
- Integritet: Uautorisert endring av informasjon skal forhindres, all endring skal kunne spores.
- Tilgjengelighet: Informasjonen skal kunne nås av de som er autorisert til det når de har behov for det.

Mens både konfidensialitet, kvalitet og tilgjengelighet vil være elementer i informasjonssikkerheten for denne VK-tjenesten, vil informasjonens integritet i svært liten grad være truet i en slik tjeneste.

3.1 Krav til informasjonssikkerhet

Kapittel 2 i personopplysningsforskriften [16] omhandler informasjonssikkerhet og stiller en del krav til sikkerheten i system der behandling av personopplysninger helt eller delvis skjer med elektroniske hjelpemidler. Disse kravene presenteres i sin helhet i forprosjektrapporten [3]. I det følgende kommenteres bare de kravene som er relevante for akkurat denne tjenesten.

§ 2-10. Fysisk sikring

Det skal treffes tiltak mot uautorisert adgang til utstyr som brukes for å behandle personopplysninger.

Utstyret er i dette tilfelle VK-enhetene. Med tanke på konfidensialitet, så lagres det ingen sensitiv informasjon i disse enhetene, bortsett fra at VK-nummeret til samtalepartner(e) kan være forhåndslagret. Om uvedkommende får fysisk adgang til VK-utstyret kan det i verste fall bety at de kan ringe opp et forhåndslagret nummer.

Men fysisk tilgang gjør det også mulig for uvedkommende å fjerne/stjele utstyr, koble utstyret fra nettet eller endre oppsettet på noen måte, noe som kan være til hinder for autorisert tilgang til tjenesten. Endring av oppsett kan også gi dårligere kvalitet på VK-forbindelsen.

§ 2-11. Sikring av konfidensialitet

Det skal treffes tiltak mot uautorisert innsyn i personopplysninger hvor konfidensialitet er nødvendig.

Uvedkommende kan få kjennskap til sensitive personopplysninger ved å se og/eller høre VK-samtale mellom helsepersonell og pasient. Det kan bl.a. gjøres ved å være i nærheten av studio eller VK-enheter når disse er i bruk.

Det er i tillegg en teoretisk mulighet for at informasjon kan oppfanges under overføring i nettet. Denne paragrafen sier derfor også at:

Personopplysninger som overføres elektronisk ved hjelp av overføringsmedium utenfor den behandlingsansvarliges fysiske kontroll, skal krypteres eller sikres på annen måte når konfidensialitet er nødvendig.

Uten annen tilsvarende sikring innebærer dette at VK-kommunikasjonen må være kryptert.

§ 2-12. Sikring av tilgjengelighet

Det skal treffes tiltak for å sikre tilgang til personopplysninger hvor tilgjengelighet er nødvendig.

Alternativ behandling skal forberedes for de tilfeller der informasjonssystemet er utilgjengelig for normal bruk.

Tilgjengelig VK-forbindelse er ikke en nødvendighet for hjemmedialysen, de har så langt greid seg uten denne tjenesten, med telefon som et godt alternativ. Men når en slik tjeneste etableres/tilbys, skapes det en forventning om at den skal fungere innenfor de beskrevne rammer. Hvis den ikke gjør

det, blir det i det minste et irritasjonsmoment som igjen vil føre til at tjenesten ikke blir benyttet. Det bør derfor foreligge rutiner for hva brukerne skal gjøre ved ulike typer feil i systemet.

§ 2-14. Sikkerhetstiltak

Sikkerhetstiltak skal hindre uautorisert bruk av informasjonssystemet og gjøre det mulig å oppdage forsøk på slik bruk.

Forsøk på uautorisert bruk av informasjonssystemet skal registreres.

Det innebærer at det må finnes en logg for bruken av systemet, og loggene bør være tilgjengelig for rutinemessig gjennomgang.

3.2 Risikovurdering

Før man starter elektronisk behandling av helseopplysninger, for eksempel kommunikasjon av helseopplysninger via videokonferanse, skal det gjennomføres risikovurdering (Personopplysningsforskriften § 2-4) [16]. Hensikten med risikovurderingen er å avdekke potensielle trusler mot informasjonens sikkerhet. Det gjøres en systematisk gjennomgang av både den tekniske løsningen og organisatoriske rutiner og prosedyrer for å gi et mest mulig riktig bilde av om tjenesten holder et forsvarlig risikonivå. Hvis man avdekker risiko som er uakseptabel, må man sette inn målrettede tiltak. Risikovurderingen skal også ta hensyn til lokale forhold, som utforming av rommet/lokalet der videokonferanseutstyret står, både hos pasienten og på sykehuset.

Risikovurderingen, gjennomført høsten 2012, er oppsummert i dette kapitlet og dokumentert i sin helhet i vedleggene B og C.

3.2.1 Metode

Risikoanalyseprosessen kan deles inn i fem faser [17]:

1. Identifisering av det som skal analyseres: system, tjeneste, omgivelser, bruk, avgrensning
2. Kartlegging av trusler[5]
3. Analyse av truslene mhp. konsekvens og sannsynlighet
4. Evaluere risikonivå
5. Foreslå tiltak som reduserer risikonivå

Trusselkartleggingen blir som oftest gjennomført i form av en ”brainstorming” i møte med dem som best kjenner til tjenesten, systemet og bruken av det. Resultatet dokumenteres fortløpende i en tabell. Trusseltabellen for denne aktuelle risikovurderingen finnes i Vedlegg C. Analyse av truslene, med vurdering av konsekvens og sannsynlighet for hver enkelt trussel, gjøres i etterkant, vanligvis i et nytt møte.

På forhånd er man blitt enig om definisjoner for konsekvens, sannsynlighet og risiko, og hva som er akseptabel risiko. – Definisjonene som er brukt i denne analysen, finnes i avsnitt B.2 i vedlegg B.

Risiko defineres som produktet av konsekvens og sannsynlighet. Når vi gjennomfører en *kvalitativ* risikovurdering, bruker vi en todimensjonal matrise som hjelpemiddel til å illustrere risiko som kombinasjon av konsekvens og sannsynlighet.

De ulike risikonivåene har vi definert på følgende måte:

Lav 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 Kan være en akseptabel risiko, men hver trussel må vurderes spesielt. Utviklingen av risikoen må overvåkes nøye og det må vurderes om risikoreduserende tiltak enkelt kan iverksettes.

Høy Uakseptabel risiko. Tjenesten kan ikke tas i bruk før risikoreduserende tiltak er iverksatt.

[5] En trussel er ethvert forhold som har potensial til å forårsake en uønska hendelse.

3.2.2 Resultater

Risikovurderingen som oppsummeres her har generell gyldighet for videokommunikasjon knyttet opp mot hjemmedialyse, der dedikerte VK-enheter benyttes hjemme hos pasienten. PC-baserte VK-løsninger vil kunne innebære et litt annet risikobilde.

3.2.2.1 Akseptkriterier

Akseptkriteriene sier noe om (u-)akseptabel risiko for trusler mot tjenesten og systemet, og trusler forårsaket av tjenesten/systemet. Her er det verdt å huske at det å akseptere risikoen betyr ikke at man aksepterer den uønska hendelsen, sikkerhetsbruddet. – De følgende akseptkriteriene kan ha gyldighet for ulike typer videokonferansetjenester.

Det er ikke akseptabelt:

- at sannsynligheten for at en pasient dør eller får varig helsetap som en følge av at denne tjenesten blir brukt, er *større* enn sannsynligheten for at pasienten dør eller får varig helsetap hvis tjenesten ikke blir brukt
- at sannsynligheten er *svært stor* for at uvedkommende *helsearbeidere* får innsyn i (ser og hører) helseinformasjonen som overføres
- at sannsynligheten er mer enn *middels* for at "allmennheten" får innsyn i (ser og hører) helseinformasjonen som overføres

  Med uvedkommende menes alle unntatt de som er i et direkte behandlingsforhold til pasienten.
- at det skjer flere ganger på rad[6] at kvaliteten er så dårlig at informasjonen blir mangelfull eller misvisende.
- at en igangsatt videokonferanse blir avbrutt i mer enn femten minutter, og at dette skjer oftere enn hver tredje gang tjenesten brukes. Dvs. mer en *middels* sannsynlighet for at dette skjer.
- at det er mer enn *middels* sannsynlighet for at videokonferanse ikke kan gjennomføres når man trenger det (at det skjer oftere enn hver tredje gang tjenesten skal brukes).

3.2.2.2 Analyse av risiko

I risikovurderingen av den aktuelle tjenesten ble det identifisert nærmere 40 mulige trusler (se trusseltabellen i vedlegg C). Truslene ble analysert med hensyn til konsekvens og sannsynlighet, og deretter plassert i ei risikomatrise for å visualisere risikonivået til den enkelte trussel og det samlede risikobildet (se Tabell 4 i vedlegg B).

Som vi ser av matrisa i vedlegg B, er ingen trusler vurdert til å ha *høy* risiko, og ingen trusler anses å ha katastrofal konsekvens. 7 (9) trusler[7] har *middels* risiko, mens de resterende 30 er vurdert å ha *lav* risiko. Dette er en god indikasjon på at det overordna risikonivået kan anses å være lavt i VK-tjenesten for hjemmedialyse. Det lave risikonivået er også et resultat av de tiltak som allerede er gjort for å oppnå tilfredsstillende sikkerhet. **Alle truslene er analysert til å ha *akseptabel* risiko.**

En detaljert analyse av de identifiserte truslene finnes i avsnitt B.3 i vedlegg B.

Trusler mot konfidensialitet

De aller fleste truslene med *middels risiko* er relatert til konfidensialitet. Også alle truslene med *alvorlig konsekvens* omhandler konfidensialitet. Dette gjenspeiler det faktum at alt av personlig helse-informasjon er sensitiv i henhold til personopplysningsloven § 2 [14], og at helsepersonell i henhold til helsepersonelloven § 21 og 21a skal forhindre brudd på taushetsplikten [15].

---

[6] Det er vanskelig å uttale seg om et slikt akseptkriterium. Brukerne har ikke opplevd at kvaliteten er så dårlig at informasjonen blir misvisende. Men skjer det mange ganger på rad kan det nok få innvirkning på tilliten til systemet og viljen til å bruke det.

[7] To av disse truslene, k15 og k16, har i praksis *ingen* sannsynlighet, så det kan diskuteres om de burde være med i matrisa i det hele tatt.

De konfidensialitetstruslene vi har identifisert kan grovt sett grupperes i fire kategorier:

a. Opptak fra videokonferansen

   Opptak/kopi av videokonferansen vil inneholde sensitiv informasjon og det må anses som alvorlig om dette kommer uvedkommende i hende.

b. Avlytting gjennom nettilgang

   Sannsynligheten for avlytting av videooverføring i nettet anser vi som praktisk talt null, siden forbindelsen er kryptert ende-til-ende. Alt utstyr på Internett er imidlertid utsatt for ondsinnede handlinger, "hackere" som prøver å utnytte feil og svakheter i system og programvare.

c. Uvedkommende tilhørere/tilskuere

   Dette kan man oppleve hos begge parter i en videokonferanse, hjemme og på sykehuset. Dersom det befinner seg andre personer hjemme hos pasienten, utenfor kameras dekning, kan det være at helsepersonellet ikke vet om disse og sier ting som bare er ment for pasienten. På sykehuset kan uvedkommende komme inn i rommet mens videokonferansen pågår og få med seg deler av samtalen.

d. Feilringing

   Feiloppringing er et kjent fenomen ved telefonbruk, og vi må anta at det vil være vanlig også ved videokonferanser. VK-enheter kan bli oppringt av uvedkommende, enten under en pågående konferanse eller når de ikke er i bruk.

Trusler mot kvalitet

Bildekvaliteten i videokonferansen kan være dårlig på grunn av dårlig eller ustabil nettforbindelse. Kvaliteten kan variere fra gang til gang, og kan være forskjellig fra ett brukersted til et annet. I pilotprosjektet har man imidlertid ikke opplevd så dårlig bildekvalitet at tjenesten ikke kan benyttes. Dårlig bildekvalitet kan også skyldes at skjerm eller kamera er konfigurert feil, eller det kan skyldes lokale lysforhold. At lysforholdene ikke er bra nok kan ofte være tilfelle, men man kan justere dette underveis i samtalen.

Som for bildekvaliteten, kan også dårlig lydkvalitet skyldes dårlig eller ustabil nettforbindelse, men lyden er i mindre grad enn bildet påvirka av båndbredden. Dårlig lyd kan også skyldes feil plassering av mikrofon og/eller høyttaler.

Trusler mot integritet

Informasjonens integritet kan synes som et irrelevant sikkerhetsaspekt for en videokonferansetjeneste som dette, og vi identifiserte da også bare én mulig trussel som kan relateres til integritet: at uvedkommende ringer opp pasienten og utgir seg for å være helsepersonell og kan gi gal/feilaktig informasjon. Men normalt vil pasient og helsepersonell kjenne hverandre, og pasienten vil straks oppdage det hvis de blir oppringt av en ukjent på videokonferanse.

Trusler mot tilgjengelighet

Alle truslene mot tilgjengelighet har i analysen fått *lav* risiko. Det gjenspeiler det faktum at dette ikke er en tjeneste til bruk ved akutte hendelser. Om tjenesten er utilgjengelig, så tilsvarer det situasjonen slik den var før denne tjenesten ble tatt i bruk. Når tjenesten finnes vil det imidlertid være en forventning om at den skal fungere. Hvis den ikke kan brukes, kan det i verste fall føre til at pasienten må reise til sykehuset for noe som ellers kunne vært løst via videokonferanse.

3.2.2.3 Forslag til tiltak

Det er flere måter å håndtere en risiko på. Man kan:

1. Unngå risikoen (å ikke utsette seg for risikoen, f.eks. ved å ikke gjennomføre det som kan føre til den uønska hendelsen)
2. Redusere risikoen (redusere sannsynlighet og/eller konsekvens)
3. Overføre risikoen (f.eks. ved å tegne en forsikring overføres risikoen til forsikringsselskapet)
4. Akseptere risikoen (leve med den, beholde den)

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. Enkle og billige tiltak som kan redusere en akseptabel risiko bør gjerne iverksettes.

Ingen trusler er vurdert å ha *uakseptabel* risiko. En medvirkende grunn til det er at mange sikkerhetstiltak allerede er satt i verk. Det er likevel en rekke enkle tiltak som kan og bør gjennomføres for å holde risikoen på et lavest mulig nivå. Blant tiltakene finnes både praktiske, organisatoriske tiltak, og tiltak som allerede er lagt inn i tjenesten.

Tiltakene kan grupperes i fire hovedkategorier.

- Prosedyrer og rutiner

  Det er viktig å ha tydelige prosedyrer/rutiner både for installasjon av utstyr, for gjennomføring av videokonferansen og for problemhåndtering og feilrapportering. En enkel brukerveiledning for alle kommunikasjonspartnere bør være en del av dette.

- Opplæring

  Det er nødvendig med en viss opplæring for både helsepersonell og pasienter/brukere hjemme. I tillegg til å lære partene opp i bruken av videokonferansetjenesten, er det nyttig med en bevisstgjøring i forhold til informasjonssikkerhet og personvern og gi en begrunnelse for de sikkerhetstiltak som er iverksatt.

- Fysiske tiltak

  Fysiske tiltak vil være en del av opplæringa av begge parter, som f.eks. tiltak for å oppnå best mulig kvalitet på lyd og bilde (dvs. optimal plassering av kamera og skjerm i forhold til lyskilder, og plassering av mikrofon i forhold til høyttaler). Fysiske tiltak omfatter også tiltak for å hindre at uvedkommende ser og/eller hører det som kommuniseres.

- Konfigurering av utstyr

  Dette er stort sett tiltak som gjøres ved installasjon av utstyret, slik som å sørge for at muligheten for autosvar er avslått og at kun krypterte samtaler skal aksepteres.

Flere detaljer om konkrete tiltak er gitt i Tabell 5 i avsnitt B.4 i vedlegg B.

4 Oppsummering

På basis av gjennomført risikovurdering og diskusjon av relevante juridiske problemstillinger er hovedkonklusjonen at videokonferansestøtte fullt forsvarlig kan tilbys pasienter som tar hjemmedialyse. Risikovurderingen har generell gyldighet for videokommunikasjon der dedikerte VK-enheter benyttes hjemme hos pasienten. PC-baserte VK-løsninger vil kunne innebære et litt annet risikobilde.

Det er imidlertid en del tiltak som kan bidra til å sikre at eventuelle risikomomenter fjernes eller minimaliseres, slik at kvaliteten av tjenesten blir optimal. Disse tiltakene er omtalt underveis i rapporten og er nedfelt i veilederen i vedlegg A.

Veilederen er tenkt som er verktøy for de som skal samarbeide om hjemmedialyse med videokonferansestøtte. Formålet er å sikre at juridiske og sikkerhetsmessige forhold blir ivaretatt så godt som over hode mulig i den daglige driften og til beste for pasienten.

Referanser

1. Arild E: ”Forprosjekt: Kartlegge behov for nye telemedisinske løsninger hjem til nyresviktpasienter.” Rapport. InnoMed 2009. http://www.innomed.no/media/media/filer_private/2011/03/02/hjemmedialyse_sluttrapport.pdf (sett 14.12.2012)
2. Rygh E, Arild E, Johnsen E, Rumpsfeld M: “Choosing to live with home dialysis-patients' experiences and potential for telemedicine support: a qualitative study.” *BMC Nephrology* 2012, 13:13. http://www.biomedcentral.com/1471-2369/13/13 (sett 14.12.2012)
3. Arild E. et al.: ”NyTTeHjem – Nye telemedisinske tjenester til hjemmedialysepasienter.” Prosjektrapport. NST-rapport 01-2012. ISBN 978-82-8242-029-7. < ev. link >
4. ITTS – Implementing Transnational Telemedicine Solutions. EU project, Northern Periphery Programme. http://www.transnational-telemedicine.eu/ (sett 14.12.2012)
5. Hogenbirk JC, Liboiron-Grenier L, Pong RW, Young NL: “How Can Telehomecare Support Informal Caregiving? Examining What is Known and Exploring the Potential.” Report, Centre for Rural and Northern Health Research, Laurentian University. May 31, 2005 http://ruralontarioinstitute.ca/file.aspx?id=ceaead3c-27d4-4450-a376-10f93cded24a (sett 14.12.2012)
6. Datatilsynet: ”Strategi for godt personvern i helsesektoren.” 30. juni 2011. http://www.datatilsynet.no/Global/04_planer_rapporter/helsesstrategi_NOV2011.pdf (sett 14.12.2012)
7. Christiansen EK, Nohr LE: ”Juridiske aspekter ved bruk av telemedisin i desentralisering av spesialisthelsetjenester.” NST-rapport 03-2011, ISBN: 978-82-8242-025-9 http://telemed.custompublish.com/juridiske-aspekter-ved-bruk-av-telemedisin-i-desentralisering-av-spesialisthelsetjenester.4558105-48869.html (sett 14.12.2012)
8. Rundskriv I-12/2001: ”Telemedisin og ansvarsforhold (ansvarsrundskrivet).” Sosial- og helsedepartementet 2001 http://www.regjeringen.no/nb/dep/hod/dok/rundskriv/2001/i-122001.html?id=108946 (sett 14.12.2012)
9. LOV-1999-07-02-61 Lov om spesialisthelsetjenesten m.m. (Spesialisthelsetjenesteloven) http://www.lovdata.no/all/hl-19990702-061.html (sett 14.12.2012)
10. Ot.prp. nr. 10 (1998-99) Om lov om spesialisthelsetjenesten m.m. Sosial- og helsedepartementet 13. november 1998 http://www.regjeringen.no/nb/dep/hod/dok/regpubl/otprp/19981999/otprp-nr-10-1998-99-.html?id=159380 (sett 14.12.2012)
11. Befring AK, Ohnstad B: ”Helsepersonelloven; med kommentarer.” 3. utgave, Fagbokforlaget, Bergen, 2010, s. 82-83
12. LOV-1999-07-02-63 Lov om pasient- og brukerrettigheter (pasient- og brukerrettighetsloven) [pasientrettighetsloven]. http://www.lovdata.no/all/hl-19990702-063.html (sett 14.12.2012)
13. LOV-2001-05-18-24 Lov om helseregistre og behandling av helseopplysninger (Helseregisterloven). http://www.lovdata.no/all/hl-20010518-024.html (sett 12.12.2012)
14. LOV-2000-04-14-31 Lov om behandling av personopplysninger (Personopplysningsloven). http://www.lovdata.no/all/hl-20000414-031.html (sett 12.12.2012)
15. LOV-1999-07-02-64 Lov om helsepersonell m.v. (Helsepersonelloven). http://www.lovdata.no/all/hl-19990702-064.html (sett 12.12.2012)
16. FOR 2000-12-15 nr 1265: Forskrift om behandling av personopplysninger (Personopplysningsforskriften). http://www.lovdata.no/for/sf/fa/xa-20001215-1265.html (sett 12.12.2012)
17. NST Faktaark nr.1 2011: Risikovurdering av informasjonssikkerhet. http://www.telemed.no/getfile.php/1738704.357.fbweevxrae/NST_Faktaark_nr_1_2011_web.pdf (sett 14.12.2012)

Vedlegg A Videokonferansestøtte for hjemmedialyse. Sjekkliste (veileder)

Vedlegget inneholder to lister, den ene for helsepersonellet på sykehussiden (A1) og den andre for pasienten og de som er sammen med pasienten (A2).

A1 Sjekkliste for sykehusets helsepersonell

Listen er organisert kronologisk med separate tabeller for de ulike fasene:

1. Planleggingsfasen, før videokonferansestøtte iverksettes
2. Ved starten av hver enkelt videokonferanse
3. Underveis i hver enkelt videokonferanse
4. Ved avslutningen av hver enkelt videokonferanse

I tabellens venstre kolonne beskrives hva som skal gjøres, utdypende forklaring i høyre kolonne.

A1.1: Før videokonferansestøtte iverksettes	
HVA SKAL GJØRES FRA SYKEHUSETS SIDE?	**UTDYPENDE KOMMENTARER**
Beskrive tjenesten og avklare ansvarsforhold • Hvem skal være involvert? - Pasienten? - Pårørende? - Helsepersonell fra UNN - Kommunalt helsepersonell? - Andre? • Avklare hvem av disse som skal gjøre hva • Diskutere og klargjøre ansvar - Sykehuset har overordnet ansvar for pasientbehandlingen. Veilederansvar. - Pasientens (ev. pårørendes) ansvar - Lokalt helsepersonell har medhjelperansvar	Dette bør alle som er involvert være med på å diskutere samtidig før første VK. Formålet med det er å sikre at alle har den samme oppfatning av hva tjenesten skal bestå i, hvem som skal gjøre hva og hva slags ansvar de forskjellige har. Dette er et ledd i arbeidet med å sikre forsvarligheten av tilbudet, jf. rapportens pkt.2.1.
Opplæring av brukere av VK-tjenesten • Bruk av VK-løsningen (teknisk/praktisk) - Gjennomgang av oppsett - Hva kan gå galt? Hva gjør man da? Ansvarsfordeling - Informasjon om innebygde/tekniske sikkerhetstiltak. • Bevisstgjøring om personvern, begrunnelse for sikkerhetstiltak. - Informasjon om praktiske sikkerhetstiltak. Særlig fokus på tiltak som er begrunnet i hensynet til taushetsplikt	Slik opplæring av pasient og andre involverte på pasientens side skal finne sted før første VK. Noe av den praktiske opplæringen bør gjøres hjemme hos pasienten i forbindelse med installasjon av VK-utstyret. Opplæring må også gis til ev. nye ansatte som skal involveres i denne tjenesten. Den viktigste begrunnelsen for gode sikkerhetstiltak er hensynet til pasientens rett til privatlivets fred og helsepersonellets taushetsplikt. Opplysninger om pasienten skal ikke havne på avveier! • Tekniske sikkerhetstiltak: - Kryptert forbindelse - Automatisk svar er slått av - Sterke passord for tilgang utenfra • Praktiske sikkerhetstiltak: - Skjerm plassert så innsyn hindres - Kamera plassert slik at bare det nødvendige vises - Bruke headset hvis andre ikke skal høre hva som sies - Presentere/vise alle som er til stede - Besvare anrop bare fra kjente nummer
Teknisk tilpasning på sykehussiden • Legge inn VK-nr/adresse til ny pasient som forhåndslagret nr i adresselista • Brukeropplæring/trening	Det forutsettes at VK-enhet allerede er installert og riktig konfigurert på sykehusavdelingen. Dvs: • Automatisk svar er slått AV • Kryptering satt som obligatorisk for videokonferanse • Sterke passord for fjernaksess • Mulighet for web-snapshots på VK-enheten er slått av Det forutsettes også at sykehuset har dedikerte personer til installasjon, brukeropplæring og support hos pasienten.

A1.2: Ved start av videokonferanse	
HVA SKAL GJØRES FRA SYKEHUSETS SIDE?	**UTDYPENDE KOMMENTARER**
Markere rommet som "opptatt" mens VK pågår / informere omgivelsene om bruk	Formålet er å hindre at uvedkommende kommer inn på rommet mens VK pågår.
Besvare anrop bare fra kjente eller forventa nummer/adresser og bare etter avtale	
Sjekke at det er klart for VK, f.eks. at det ikke er en tidligere VK som ikke er nedkoblet	Dette oppdages straks man prøver å kople opp.
Spørre pasienten hvem som er til stede, og presentere eventuelle andre som er sammen med helsepersonell	Gjøres rutinemessig ved oppstart.
Sjekke at kameraet er slik plassert at man ser det man trenger for en forsvarlig tjeneste, men ikke mer	Gjøres rutinemessig ved oppstart. Helsepersonell kan be om at pasientens kamera flyttes på, eller kamera kan fjernstyres.
Vurdere om skjermen kan ses av uvedkommende og justere iht. det	Gjøres rutinemessig ved oppstart.

A1.3: Underveis i videokonferansen	
HVA SKAL GJØRES FRA SYKEHUSETS SIDE?	**UTDYPENDE KOMMENTARER**
Vurdere om VK har god nok kvalitet til at riktige/nødvendige avgjørelser kan tas	Ser man de detaljene man ønsker å se, og hører man godt nok?
Si ifra om dårlig bilde og/eller lyd og justere underveis	F.eks. slå av/på lys, endre plassering av kamera og mikrofon, justere lydvolum. Hvis kvaliteten blir for dårlig, kan man bli enig om f.eks.: • Prøve å kople ned VK og starte på nytt • Bruke telefon når lyden på VK er for dårlig
Tilpasse lydnivået slik at utenforstående ikke hører hva som sies, ev. vurdere bruk av headset	Headset kan bidra til at lyden ikke settes for høyt og også bidra til at helsepersonellet ikke snakker høyere enn nødvendig i konferansen.
Håndtere forstyrrelser som f.eks. innkommende telefonsamtaler eller at andre kommer inn i rommet.	Man kan f.eks.: • La være å ta telefonen mens VK pågår • Stenge VK-mikrofon hvis telefonen må besvares

A1.4: Ved avslutning av videokonferanse	
HVA SKAL GJØRES FRA SYKEHUSETS SIDE?	**UTDYPENDE KOMMENTARER**
Kople ned forbindelsen når videokonferansen er ferdig	Avslutte, "legge på" – ikke bare slå av skjermen.

A2 Sjekkliste for pasientsiden av konferansen

Listen er organisert kronologisk med separate tabeller for de ulike fasene:

1. Planleggingsfasen, før videokonferansestøtte iverksettes
2. Ved starten av hver enkelt videokonferanse
3. Underveis i hver enkelt videokonferanse
4. Ved avslutningen av hver enkelt videokonferanse

I tabellen beskrives hva som skal gjøres, med noe utdypende forklaring i høyre kolonne.

A2.1: Før videokonferansestøtte iverksettes	
HVA SKAL GJØRES PÅ PASIENTENS SIDE?	**UTDYPENDE KOMMENTARER**
Få informasjon om tjeneste og ansvarsforhold • Hvem skal være involvert: - Pasienten - Pårørende? - Helsepersonell fra UNN - Kommunalt helsepersonell? - Andre? • Avklare hvem av disse som skal gjøre hva • Diskutere og klargjøre ansvar - Sykehuset har overordnet ansvar for pasientbehandlingen. Veilederansvar. - Pasientens (ev. pårørendes) ansvar - Lokalt helsepersonell har medhjelperansvar	Dette bør alle som er involvert være med på å diskutere samtidig, før første VK. Formålet med det er å sikre at alle har den samme oppfatning av hvem som skal gjøre hva og hva slags ansvar de forskjellige har.
Opplæring av de involverte • Bruk av VK-løsningen (teknisk/praktisk) - Gjennomgang av oppsett - Hva kan gå galt? Hva gjør man da? - Ansvar og oppgaver - Informasjon om innebygde tekniske sikkerhetstiltak. • Bevisstgjøring om personvern (begrunnelse for tiltak). - Informasjon om praktiske sikkerhetstiltak.	Opplæringen skal finne sted før første VK. En del av den praktiske opplæringen, trening i å bruke VK-utstyret, bør gjøres hos pasienten i forbindelse med installasjon av utstyr. Sikkerhetstiltak i systemet: • Teknisk: - Kryptert forbindelse - Automatisk svar slått av - Sterke passord for tilgang utenfra • Praktisk: - Plassering av skjerm i forhold til innsyn - Bruke headset hvis andre ikke skal høre hva som sies - Kameraets dekningsområde - Presentere/vise alle som er til stede - Besvare anrop bare fra kjente nummer - Slå av VK-enhet når den ikke brukes
Installasjon av VK-utstyr og ansvar for oppfølging • Automatisk svar slås AV • Sette kryptering som obligatorisk for videokonferanse • Bruke sterke passord for fjernaksess • Slå av mulighet for web-snapshots på VK-enheten • Lage adresseliste (legge inn forhåndslagrede nummer) • Konfigurere skjerm og kamera for optimalt bilde • Plassere skjermen slik at utenforstående ikke ser hva som vises bildet • Finne optimal plassering av mikrofon • Brukeropplæring/trening • Informere om support/hjelp	Utføres av tjenestetilbyder (UNN) v/ teknisk personell. Der det er naturlig gjøres dette sammen med pasienten og ev. andre personer på pasientens side.

A2.2: Ved start av videokonferanse	
HVA SKAL GJØRES PÅ PASIENTENS SIDE?	**UTDYPENDE KOMMENTARER**
Ta stilling til om rommet skal skjermes for andres innsyn mens VK pågår	Dersom rommet skal skjermes: • Lukke døra • Si ifra til andre at de ikke skal komme inn i rommet
Besvare anrop bare fra kjente nummer/ adresser og bare etter avtale	For å ivareta privatlivets fred – forhindre oppringing fra uvedkommende.
Fortelle hvem som er til stede i rommet, presentere de andre	Gjøres rutinemessig ved oppstart
Sjekke at kameraet er slik plassert at man viser det helsepersonellet trenger å se, men ikke mer	Gjøres rutinemessig ved oppstart. Helsepersonellet på sykehussiden må ev. si ifra om kameraet må plasseres annerledes.
Vurdere om skjermen kan ses av uvedkommende og justere i forhold til det	Gjøres rutinemessig ved oppstart.

A2.3: Underveis i videokonferansen	
HVA SKAL GJØRES PÅ PASIENTENS SIDE?	**UTDYPENDE KOMMENTARER**
Si ifra om dårlig bilde og/eller lyd og justere underveis	F.eks. slå av/på lys, endre plassering av kamera og mikrofon, justere lydvolum. Hvis kvaliteten blir for dårlig, kan man bli enig om f.eks.: • Prøve å kople ned VK og starte på nytt • Bruke telefon når lyden på VK er for dårlig
Tilpasse lydnivået slik at utenforstående ikke hører hva som sies, eller vurdere å bruke headset	Headset kan bidra til at lyden ikke settes for høyt og også bidra til at pasienten ikke snakker høyere enn nødvendig i konferansen.
Håndtere forstyrrelser som f.eks. innkommende telefonsamtaler eller at andre kommer inn i rommet.	Man kan f.eks.: • La være å ta telefonen mens VK pågår • Stenge VK-mikrofon hvis telefonen må besvares

A2.4: Ved avslutning av videokonferanse	
HVA SKAL GJØRES PÅ PASIENTENS SIDE?	**UTDYPENDE KOMMENTARER**
Kople ned forbindelsen når videokonferansen er ferdig	Avslutte, ”legge på” – ikke bare slå av skjermen.
Slå av VK-utstyret når det ikke er i bruk	For å unngå uønsket oppringing

Vedlegg B Rapport fra risikovurdering

Før man starter elektronisk behandling av helseopplysninger, for eksempel kommunikasjon av helseopplysninger via videokonferanse, skal det gjennomføres risikovurdering (Personopplysningsforskriften § 2-4). Hensikten med risikovurderingen er å avdekke potensielle trusler mot informasjonens sikkerhet. Det gjøres en systematisk gjennomgang av både den tekniske løsningen og organisatoriske rutiner og prosedyrer for å gi et mest mulig riktig bilde av om tjenesten holder et forsvarlig risikonivå. Hvis man avdekker risiko som er uakseptabel, kan man sette inn målrettede tiltak. Risikovurderingen må også ta hensyn til lokale forhold, som utforming av rommet/lokalet der videokonferanseutstyret står, både hos pasienten og på sykehuset.

Risikovurderingen, gjennomført høsten 2012, er dokumentert i dette vedlegget og i vedlegg C. En oppsummering er gitt i kapittel 3 i rapporten.

B.1 Metode og gjennomføring

Risikoanalyseprosessen kan deles inn i fem faser [17]:

1. Identifisering av det som skal analyseres: system, tjeneste, omgivelser, bruk, avgrensning
2. Kartlegging av trusler[8]
3. Analyse av truslene mhp. konsekvens og sannsynlighet
4. Evaluere risikonivå
5. Foreslå tiltak som reduserer risikonivå

Tjenesten som er analysert, er beskrevet i avsnitt 1.3 foran.

Trusselkartleggingen ble i hovedsak gjennomført i et 3-timers møte med ”brainstorming” 25.09.2012. Supplerende informasjon ble innhentet gjennom e-post og intervju. Analyse av truslene, med vurdering av konsekvens og sannsynlighet for hver enkelt trussel, ble gjort i etterkant av dette møtet og i et nytt møte 21.11.2012. Her deltok:

Deltakere i risikovurderingen:

- Merja H. Mourujärvi, Åse Lauritzen og Marit Solbu fra Nyremedisinsk avdeling, Medisinsk klinikk, UNN
- Stig Karoliussen, Eli Arild, Ellen K. Christiansen fra NST
- Leder av risikovurderingen: Eva Henriksen, NST

[8] En trussel er ethvert forhold som har potensial til å forårsake en uønska hendelse.

B.2 Definisjoner av konsekvens, sannsynlighet og risiko

Vi bruker kvalitative verdier på *konsekvens*, *sannsynlighet* og *risikonivå*. Verdiene vi bruker er definert i de følgende avsnittene.

B.2.1 Konsekvens

Vi har valgt å ha fire nivå for konsekvens, definert ut fra ulike kriterier for virksomheten (UNN) og for den/de aktuelle pasienten(e). Tabell 1 viser vår definisjon av verdiene for konsekvens.

Tabell 1: Definisjon av verdier for Konsekvens

	Virksomheten (UNN), prosjektet			Person/Pasient		
Konsekvens	**Lov**	**Økonomi**	**Anseelse**	**Liv/helse**	**Økonomi**	**Anseelse, rykte**
Liten	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	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, forbigående virkning på helse	Økonomisk tap, kan gjen-opprettes	Tap av anseelse, kompromit-tering av opplysninger av mindre alvorlig type
Alvorlig	Alvorlig lovbrudd, mindre straff/bøter	Stort økonomisk tap, opp-rettelig	Alvorlig tap av anseelse, lengre virkning på tillitt og respekt	Redusert helse	Stort økonomisk tap, opprettelig	Alvorlig tap av anseelse, kompromit-tering av sensitive og krenkende opplysninger
Katastrofal	Alvorlig lovbrudd, straff/bøter	Betydelig, økonomisk tap, uopp-rettelig	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

B.2.2 Sannsynlighet

Ulike måter å definere sannsynlighetsnivåene på er vanlig, bl.a. ut fra:

Frekvens eller hyppighet: Antall ganger en trussel forventes å inntreffe i forhold til antall ganger en tjeneste brukes, eller: antall ganger en trussel forventes å inntreffe i en gitt tidsperiode

Tiltak: Om det er iverksatt tiltak mot kjente sårbarheter, og i hvilken grad tiltakene fungerer

Letthet: Hvor lett det er å bryte sikkerheten (utløse en trussel) for interne og eksterne personer (uaktsomhet, forsett og overlegg)

Motivasjon: Sannsynlighet basert på brukerens motivasjon og hvor interessant systemet/tjenesten eller informasjonen er

Vi har valgt å ha fire nivå også for sannsynlighet, se Tabell 2.

Tabell 2: Definisjon av verdier for Sannsynlighet

Sannsynlighet	Frekvens	Sårbarhet Tiltak	Letthet/Vanskelighetsgrad Motivasjon
Liten	Hver 50. oppkopling/ kommunikasjon eller sjeldnere	Sikkerhetstiltak er etablert og fungerer etter hensikten	Må ha detaljkunnskap om systemet. Trenger spesielle hjelpemidler. Brudd kan bare skje med overlegg, bevisst.
Middels	Oftere enn hver 50. men sjeldnere enn hver 10. oppkopling/ kommunikasjon	Sikkerhetstiltak er etablert og fungerer etter hensikten	Brudd kan skje med normal kjennskap til systemet. Vanlige hjelpemidler. Med overlegg, bevisst.
Stor	Oftere enn hver 10. oppkopling/ kommunikasjon	Sikkerhetstiltak er ikke fullt etablert eller de fungerer ikke etter hensikten	Brudd 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.
Svært stor	Annenhver eller hver oppkopling/ kommunikasjon	Sikkerhetstiltak er ikke etablert	Brudd kan skje uten kjennskap til systemet. Uten hjelpemidler. Ved uaktsomhet eller feil bruk. Med overlegg hvis noen er villig til å betale for informasjonen.

B.2.3 Risiko

Risiko er definert som produktet av konsekvens og sannsynlighet. Når vi bruker kvalitative verdier, bruker vi ei todimensjonal matrise som verktøy, der produktet illustreres som kombinasjonen av trusselens konsekvens og sannsynlighet.

Matrisa under (Tabell 3) viser definisjon av de ulike risikonivå vi har valgt å benytte for denne risikovurderingen. Vi har her valgt å bruke tre risikonivå: Lav, Middels, Høy.

Tabell 3: Risikomatrise og definisjon av verdier for Risiko

Kons. / Sanns.	Liten	Moderat	Alvorlig	Katastrofal
Liten	Lav	Lav	Middels	Høy
Middels	Lav	Middels	Middels	Høy
Stor	Lav	Middels	Høy	Høy
Svært stor	Middels	Middels	Høy	Høy

De ulike risikonivåene har vi definert på følgende måte:

Lav 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 Kan være en akseptabel risiko, men hver trussel må vurderes spesielt. Utviklingen av risikoen må overvåkes nøye og det må vurderes om risikoreduserende tiltak enkelt kan iverksettes.

Høy Uakseptabel risiko. Tjenesten kan ikke tas i bruk før risikoreduserende tiltak er iverksatt.

B.2.4 Akseptkriterier

Akseptkriteriene våre sier noe om (u-)akseptabel risiko for trusler mot tjenesten og systemet, og trusler forårsaket av tjenesten/systemet, i første rekke om (u-)akseptabel konsekvens. De følgende akseptkriteriene ble diskutert i risikovurderingen.

Det er ikke akseptabelt:

- at sannsynligheten for at en pasient dør eller får varig helsetap som en følge av at denne tjenesten blir brukt, er *større* enn sannsynligheten for at pasienten dør eller får varig helsetap hvis tjenesten ikke blir brukt
- at sannsynligheten er svært stor for at uvedkommende *helsearbeidere* får innsyn i (ser og hører) helseinformasjonen som overføres
- at sannsynligheten er mer enn middels for at "allmennheten" får innsyn i (ser og hører) helseinformasjonen som overføres

  Med uvedkommende menes alle unntatt de som er i et direkte behandlingsforhold til pasienten.
- at det skjer flere ganger på rad[9] at kvaliteten er så dårlig at informasjonen blir mangelfull eller misvisende.
- at en igangsatt videokonferanse blir avbrutt i mer enn femten minutt, og at dette skjer oftere enn hver tredje gang tjenesten brukes. Dvs. mer en *middels* sannsynlighet for at dette skjer.
- at det er mer enn *middels* sannsynlighet for at videokonferanse ikke kan gjennomføres når man trenger det (at det skjer oftere enn hver tredje gang tjenesten skal brukes).

B.3 Trusselkartlegging og analyse

Truslene, som ble identifisert gjennom møte med personell i Nyremedisinsk avdeling og personell fra NST, er listet opp i trusseltabellen i vedlegg C. Verdier for sannsynlighet, konsekvens og risikonivå er satt inn i tabellen. Totalt ble det identifisert 39 mulige trusler. Truslene er entydig identifisert med en kombinasjon av bokstaver og tall. Bokstavene angir hvilket av sikkerhetsaspektene konfidensialitet (k), kvalitet (q), integritet (i) og tilgjengelighet (t) trusselen er relatert til, og fortløpende nummerert innenfor hver av disse kategoriene.

Truslene er plassert i risikomatrisa (Tabell 4) for å visualisere risikonivået til den enkelte trussel og det samlede risikobildet.

Som vi ser av matrisa er ingen trusler vurdert til å ha *høy* risiko, og ingen trusler anses å ha katastrofal konsekvens. 7 (9) trusler[10] har *middels* risiko, mens de resterende 30 er vurdert å ha *lav* risiko. Dette er en god indikasjon på at det overordna risikonivået kan anses å være lavt i VK-tjenesten for hjemmedialyse. Det lave risikonivået er også et resultat av de tiltak som allerede er gjort for å oppnå tilfredsstillende sikkerhet. Alle truslene er analysert til å ha *akseptabel* risiko.

---

[9] Det er vanskelig å uttale seg om et slikt akseptkriterium. Brukerne har ikke opplevd at kvaliteten er så dårlig at informasjonen blir misvisende. Men skjer det mange ganger på rad kan det nok få innvirkning på tilliten til systemet og viljen til å bruke det.

[10] To av disse truslene, k15 og k16, har i praksis *ingen* sannsynlighet, så det kan diskuteres om de burde være med i matrisa i det hele tatt.

Tabell 4: Risikomatrise for Hjemmedialysetjenesten

Kons. / Sanns.	Liten	Moderat	Alvorlig	Katastrofal
Liten	k6b, k7, k9, k11, k14, q2, q4, q6, q10, i1, t1, t2, t7	k2, k3, k13 t3, t4, t5	(k15, k16), k17, k18, k19, k20	
Middels	k8, k10 q1, q5 t6	k12 q3		
Stor	k1, k4, k5 q7, q8, q9			
Svært stor	k6			

I de neste avsnittene analyseres de enkelte truslene mot sikkerhetsaspektene konfidensialitet, kvalitet, integritet og tilgjengelighet. Truslene med størst konsekvens omtales først, sammen med trusler av liknende type.

B.3.1 Trusler mot konfidensialitet

Som vi ser av risikomatrisa, er de aller fleste truslene med *middels* risiko relatert til konfidensialitet.

Opptak av samtale

Truslene **k17-k19** handler om urettmessig opptak/kopiering av videokonferansen. Slike opptak vil inneholde sensitiv informasjon og det må anses som alvorlig om dette kommer uvedkommende i hende.

Den enkleste måten å få dette til på, er at noen filmer konferansen med annet eksternt utstyr som mobiltelefon eller kamera (trussel **k18**). Dette kan være vanskelig å kontrollere, men sannsynligheten for at det skal skje i denne typen tjeneste vurderes som liten – basert på motivasjonsaspektet.

I helsenettet finnes det en opptakstjeneste for ”streaming” av videokonferanser. Dersom en av partene ved en feiltakelse ringer opp denne tjenesten (trussel **k19**), vil konferansen tas opp og gjøres tilgjengelig på Internett (http://tcs.nhn.no). Vi anser også her sannsynligheten for å være liten: brukerne må kjenne til den aktuelle adressen og kanskje ha den forhåndslagra på sin enhet for at dette skal kunne skje.

Man kan også tenke seg at selve VK-utstyret har en innebygd opptaksmulighet (trussel **k17**). Men i det utstyret som i dag brukes for denne tjenesten er det ingen slik mulighet, slik at denne trusselen vurderes som svært lite sannsynlig.

Trussel **k14**, at enkeltbilder fra video legges ut som ”web-snapshots”, er i samme kategori som de foregående, men i dette tilfellet er det bare stillbilder som legges ut, og ikke lyd. Vi anser derfor konsekvensen for å være liten om dette skulle skje, samtidig som sannsynligheten for at dette skal skje også er liten fordi funksjonen for web-snapshots er avslått i VK-enhetene. (Denne funksjonen kan slås på fra tekniker i helsenettet, bevisst eller ved en feiltakelse, men vi ser heller ikke noen større sannsynlighet for dette.) Det er i tillegg lagt inn sterke passord for fjern-aksess til VK-enhetene på pasientenes side.

Avlytting i nettet

En annen gruppe trusler omhandler muligheten for at uvedkommende skal kunne avlytte video-konferansen under overføring i nettet. Om dette skulle skje ville det anses som alvorlig. Sannsynligheten er imidlertid praktisk talt null for at dette skal skje, både i Internett (trussel **k15**) og i helsenettet (trussel **k16**), siden forbindelsen er kryptert ende-til-ende.

Alt utstyr på Internett er til en viss grad utsatt for ondsinnede handlinger, ”hackere” som utnytter feil og svakheter i programvare (trussel **k20**). I en VK-tjeneste kan det gi seg utslag i at uvedkommende overtar styring av enheten og kan se og/eller høre hva som foregår. Også dette vil ha alvorlig konsekvens, men selv om det finnes eksempel på at slikt har skjedd med annen type utstyr, anser vi sannsynligheten for svært liten for en slik hendelse i denne tjenesten.

Uvedkommende tilhørere/tilskuere hos en av partene

Trussel **k12** omhandler situasjonen at videokonferansen ikke blir avsluttet skikkelig etter endt samtale, f.eks. at bare skjermen slås av uten at forbindelsen er koplet ned. Da kan det bli sagt ting som det ikke var mening at parten i den andre enden skulle høre. Vi anser denne trusselen for å ha moderat konsekvens. Vi vet at dette er noe som ofte skjer i studio som brukes til møter og undervisning, og basert på dette vurderer vi sannsynligheten til å være middels. Vi anser likevel dette å være en akseptabel risiko, siden overholdelse av gode rutiner vil være et enkelt tiltak å gjennomføre.

Flere trusler er relatert til muligheten for at uvedkommende kan se og høre en pågående video-konferanse, det være seg hjemme hos pasienten (truslene **k1-k3**) eller på avdelingen på sykehuset (truslene **k4-k5**).

Dersom det befinner seg andre personer hjemme hos pasienten, utenfor kameras dekning, kan det være at helsepersonellet ikke vet om disse og sier ting som bare er ment for pasienten. Pasienten kan selv til en viss grad styre at sensitiv informasjon ikke gis, ved å avbryte helsepersonellet. Men det forutsetter at pasienten vet om at andre er til stede. Trussel **k1** gjelder tilfellet der pasienten vet at andre er til stede, noe vi anser for å ha liten konsekvens, selv om sannsynligheten kan være stor. De tilfellene der pasienten ikke vet at andre ser og/eller hører samtalen, enten de er i samme rom som pasienten (trussel **k2**) eller de ser og hører gjennom vinduer og dører (trussel **k3**), anser vi for å ha moderat konsekvens. Vi ser det imidlertid som lite sannsynlig at pasienten ikke vet at andre er tilstede i rommet (**k2**) eller at noen skal få med seg et sammenhengende innhold av videokonferansen ved å lytte gjennom vindu/dører (**k3**).

Trussel **k3** er også relevant for forholdene på sykehussiden. Her kan det også skje at uvedkommende kommer inn i rommet der det pågår videokonferanse (trussel **k4**). Om disse får kjennskap til sensitiv informasjon, er bl.a. avhengig av om skjermen er plassert slik at den kan ses fra døra og om lyden er så høy/tydelig at den kan høres fra avstand. Vi antar imidlertid at de som uforvarende kommer inn i rommet mens det er opptatt, vil trekke seg tilbake så raskt at de ikke får noen helhetlig informasjon. Konsekvensen er derfor vurdert til å være liten, selv om sannsynligheten for at noen kommer inn uforvarende må anses å være stor.

En lignende trussel vil være at helsepersonell mottar telefonoppringing mens de sitter i en video-konferanse med pasienten (trussel **k5**). Konsekvensen er liten, ihvertfall for den pasienten som er part i videokonferansen. Dersom telefonsamtalen handler om en (annen) pasient, kan det i verste fall føre til at pasienten på VK får kjennskap til sensitiv informasjon om den andre pasienten. Sannsynligheten er stor for at telefonoppringing vil komme, men det er mange innlysende tiltak som kan iverksettes for å hindre konfidensialitetsbrudd.

Feilringing, flere på linja

En stor gruppe trusler handler om at en VK-enhet kan bli oppringt av uvedkommende, enten under en pågående videokonferanse eller når den ikke er i bruk. En av disse truslene, **k6**, har fått *middels* risiko, de øvrige har *lav* risiko fordi konsekvensen anses som liten.

Vi har i denne tjenesten erfart at VK-enheter på Internett blir ”spammet” med oppringing fra en ukjent server på Internett (trussel **k6**). Basert på denne erfaringen har vi satt sannsynligheten for denne trusselen til å være svært stor. Siden autosvar er slått av, vil det imidlertid ikke bli etablert noen forbindelse. Konsekvensen er derfor satt til å være liten, dette er kun et irritasjonsmoment for pasienten, som ser det som en lang rekke ubesvarte anrop. Det verste for pasienten har vært at når dette f.eks. skjer om natta vil skjermen, som ellers er mørk, lyse opp.

Videokonferanseenheten på sykehuset står på helsenettet og kan ikke på samme måten ringes opp av enheter som står på Internett (trussel **k6b**). Det finnes imidlertid fortsatt en mulighet for enheter utenfra å ringe opp enheter i helsenettet via ISDN. Konsekvensen er liten fordi oppringing vil oppdages og ingen sensitiv informasjon røpes. Sannsynligheten anser vi også å være liten siden det kreves en del detaljkunnskap om denne muligheten.

VK-enhetene kan også bli oppringt fra andre VK-enheter på nettet, enten som en tilsiktet handling (trussel **k7**) eller som en feiloppringing (trussel **k8**). Enheter på helsenettet kan bare bli oppringt fra

andre enheter i samme nett[11], mens VK-enhetene hos pasientene kan bli oppringt både fra helsenettet og fra Internett. I begge tilfeller vil konsekvensen være liten fordi oppringing vil oppdages, enten det pågår videokonferanse eller ikke, og ingen sensitiv informasjon vil røpes. Vi anser sannsynligheten for en tilsiktet oppringing å være liten (- hva skulle motivere en slik handling?), mens sannsynligheten for feiloppringing fra uvedkommende vil være større, minst middels.

Feiloppringing kan også forekomme mellom de enhetene som vanligvis inngår i denne tjenesten. I alle tilfeller anser vi konsekvensen å være liten, for ingen sensitiv informasjon gis. Andre personer på sykehuset, som rettmessig bruker den samme VK-enheten, kan ved en feiltakelse ringe pasientens nummer som er forhåndslagra i enheten (trussel **k10**). Sannsynligheten for slik feilringing anses som middels. Pasienten hjemme har kanskje ingen andre forhåndslagrede nummer enn det til sykehusavdelinga. Men man kan tenke seg at tilfeldige besøkende, f.eks. barnebarn, prøver en oppringing til dette nummeret (trussel **k11**). VK-enheten på sykehuset har ikke autosvar påslått, og rommet brukes lite til andre formål. Om det skulle være noen i rommet, anser man det lite sannsynlig at de skulle velge å svare. Det samme gjelder dersom pasienten selv skulle ringe opp sykehuset utenom avtalt tidspunkt og andre er til stede i rommet (trussel **k9**)

Trussel **k13** omhandler den muligheten at helsepersonell på sykehuset ringer opp en annen pasient før videokonferansen med den forrige er koplet ned. Det vil bety at pasientene kan se og høre hverandre, konsekvensen er derfor satt til moderat, men helsepersonellet vil raskt oppdage det og kan kople ned forbindelsen. Sannsynligheten anses som liten, man vil normalt se en eventuell oppkoplet VK-enhet på skjermen før man starter.

B.3.2 Trusler mot kvalitet

Selv om kvalitet er en viktig egenskap ved videokonferanse, er det bare én av truslene mot kvalitet som har *middels* risiko (**q3**). De øvrige truslene mot kvalitet har fått *lav* risiko fordi de har liten konsekvens for denne tjenesten.

Trussel **q3** handler om at bildekvaliteten i videokonferansen er dårlig på grunn av dårlig eller ustabil nettforbindelse. Kvaliteten kan variere fra gang til gang, og kan være forskjellig fra ett brukersted til et annet – slik man har erfart i dette pilotprosjektet. Sannsynligheten er satt til å være middels. Man har i pilotprosjektet ikke opplevd så dårlig bildekvalitet at tjenesten ikke kan benyttes, men om det skulle skje anses konsekvensen å være moderat; det kan gå ut over tilliten til tjenesten og viljen til å bruke denne løsningen.

Dårlig bildekvalitet kan også skyldes at skjerm eller kamera er konfigurert feil (trussel **q2**), eller det kan skyldes lokale lysforhold (trussel **q1**). Feil konfigurering vil sannsynligvis bare være et problem ved første gangs bruk. At lysforholdene ikke er bra nok vil nok skje oftere, men man kan justere dette underveis i samtalen.

Man kan også oppleve at bilde mangler ved oppstart, at man bare har lyd (trussel **q4**), eller at man ikke ser den andre parten i bildet og f.eks. bare ser tak og vegger (trussel **q5**). Begge disse forholdene kan rettes opp når videokonferansen er startet. Kamera hjemme hos pasienten kan lett bli satt i ”feil” posisjon når VK-enheten ikke er i bruk. Kameraet kan til en viss grad fjernstyres fra sykehuset.

Den andre gruppen av trusler mot kvalitet gjelder lydkvaliteten. Som for bildekvaliteten, kan dårlig lydkvalitet skyldes dårlig eller ustabil nettforbindelse (trussel **q6**), men lyden er i mindre grad enn bildet påvirka av båndbredden. Dårlig lyd kan også skyldes feil plassering i forhold til mikrofon og/eller høyttaler (trussel **q7**) eller at mikrofonen er plassert for nær høyttaler (trussel **q8**). Slike forhold kan skje ofte, men kan lett justeres underveis i videokonferansen. Om lyden er helt borte kan det skyldes at høyttaler og/eller mikrofon ikke er slått på (trussel **q9**). Også dette kan enkelt rettes opp når videokonferansen er startet.

En siste trussel i kategorien kvalitet er at brukergrensesnittet for videokonferansen er så vanskelig at det kan misforstås eller hindre bruken av tjenesten (trussel **q10**). F.eks. kan man rote seg inn i menyer som i verste fall endrer på konfigurasjonen av utstyret (se trussel t4). I denne tjenesten er bruker-grensesnittet gjort så enkelt som mulig, det er bare å velge riktig mottaker og ringe opp. Bruker-grensesnittet kan imidlertid være med på å øke risikoen for feiloppringing (se truslene k9 g k10 foran).

[11] Unntak: Oppringing via ISDN, som nevnt ovenfor.

B.3.3 Trusler mot integritet

Informasjonens integritet kan synes som et irrelevant sikkerhetsaspekt for en videokonferansetjeneste som dette, og vi identifiserte da også bare én trussel som kan relateres til integritet:

Trussel **i1** handler om at uvedkommende ringer opp pasienten og utgir seg for å være helsepersonell og kan gi gal/feilaktig informasjon. I denne tjenesten anses dette som uaktuelt. Pasient og helsepersonell kjenner hverandre og pasienten vil straks oppdage det hvis de blir oppringt av en ukjent på videokonferanse. Det vil heller ikke bli brukt vikarer i en slik tjeneste. Trusselen har svært liten konsekvens om den inntreffer, og sannsynligheten for at en slik oppringing skal skje anses som liten. (Se også diskusjon av truslene k6-k9 foran.)

B.3.4 Trusler mot tilgjengelighet

Alle truslene mot tilgjengelighet har i analysen fått *lav* risiko. Om tjenesten er utilgjengelig, så tilsvarer det situasjonen slik den var før denne tjenesten ble tatt i bruk. Når tjenesten finnes vil det imidlertid være en forventning om at den skal fungere. Hvis den ikke kan brukes, kan det i verste fall føre til at pasienten må reise til sykehuset for noe som ellers kunne vært løst via videokonferanse.

For truslene **t1** og **t2** skyldes utilgjengeligheten at VK-utstyret er blitt stjålet, enten fra sykehuset eller fra pasienten. Vi anser dette som lite sannsynlig, VK-enhetene er antakelig ikke så lett omsettelig som f.eks. PC-er.

Truslene **t3** og **t4** handler om at videokonferansen ikke fungerer fordi konfigurasjonen er blitt endret, enten ved en feiltakelse eller som en tilsiktet handling. I verste fall gir det et dårlig inntrykk for framtidig bruk av tjenesten at slike problemer kan oppstå (moderat konsekvens), men sannsynligheten for dette anses som liten. Den samme vurdering gjelder trusselen om at utstyr ikke fungerer fordi det er ødelagt (trussel **t5**). Man har opplevd at dette skjer, men ikke ofte. I noen tilfeller kan problemet være så enkelt som at det bare er batteriet i fjernkontrollen som er gått tom for strøm (trussel **t7**).

Videokonferanse kan også være utilgjengelig i kortere eller lengre tid pga. linjebrudd/nettproblemer (trussel **t6**), dette er som oftest forhold som ligger utenfor VK-tjenestens kontroll.

B.4 Forslag til tiltak

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 (redusere sannsynlighet og/eller konsekvens – det er vanskelig å redusere konsekvens)
3. Overføre risikoen (f.eks. ved å tegne en forsikring overføres risikoen til et forsikringsselskap)
4. Akseptere risikoen (leve med den, beholde den). NB: 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.

Ingen trusler er vurdert å ha *uakseptabel* risiko. En medvirkende grunn til det er at mange sikkerhetstiltak allerede er satt i verk. Det er likevel en rekke enkle tiltak som kan og bør gjennomføres for å holde risikoen på et akseptabelt lavt nivå.

Tabell 5 lister opp en del slike tiltak og gir en oversikt over hvilke trusler de ulike tiltakene kan redusere risikoen for. Blant tiltakene finnes både praktiske, organisatoriske tiltak, og tiltak som allerede er lagt inn i tjenesten. Som tabellen viser vil flere av sikkerhetstiltakene være med på å redusere risikoen til mange trusler som hver for seg er akseptable. Disse tiltakene vil til sammen redusere den totale risikoen for systemet.

Tabell 5: Foreslåtte sikkerhetstiltak

Sikkerhetstiltak	Berørte trusler
Prosedyrer og rutiner:	
Informere samtaleparten om andre som er til stede i rommet eller som kommer inn i løpet av samtalen, presentere disse.	k1
Introdusere/presentere eventuelle nye personer/vikarer som skal være med	i1
Dempe lyden slik at utenforstående ikke hører hva som sies.	k3, k4
La være å svare telefonoppringing mens VK pågår	k5
Stenge VK-mikrofon mens telefonsamtale pågår	k5
Kople ned forbindelsen når VK avsluttes	k12, k13
Si ifra og justere lysforhold og lyd underveis	q1, q4, q7, q8, q9
Testing/utprøving under installasjon	q2
Vurdere om VK har god nok kvalitet for å ta avgjørelser	q1, q2,q3
Bruke telefon hvis VK-lyden er for dårlig	q6, q9
Opplæring:	
Ikke besvare VK-anrop fra andre enn de som er forventa	k6, k6b, k7, k8, k9, k11
Ikke ringe opp ny VK uten at den forrige er koplet ned	k13
Ikke gjøre opptak av videokonferansen på noen måte	k17, k18, k19
Kontrollere at riktig nummer ringes (forhåndslagra)	k19
Optimal lyssetting og plassering av kamera	q1, q5
Plassering av mikrofon	q7, q8
Bruk av fjernkontroll og menyer	q10, t7
Support: Oversikt over hvem som skal kontaktes ved ulike problem	t3, t4, t5, t6
Fysiske tiltak:	
Plassering av skjerm for å hindre innsyn fra vindu og dør	k3, k4
Vurdere bruk av headset	k3, k4
Markere rommet som opptatt mens VK pågår (plakat, låst dør)	k4
Slå av VK-utstyr nå det ikke er i bruk.	k6, k10
Fjernstyre kamera hos pas. for å få optimalt bilde	q1, q2, q5
Kople ned VK og kople opp på nytt ved visse problemer	q3, q6
Konfigurasjon av utstyr:	
Autosvar avslått	k6, k6b, k7, k8, k9, k11
Sterke passord for fjernaksess via web el. l.	k14
Slå av mulighet for ”web-snapshots” på VK-enheten	k14
Obligatorisk ende-til-ende-kryptering av VK	k15, k16
Forhåndslagrede nummer	k19
Optimal konfigurering av skjerm og kamera	q2
Oppdatering av programvare, patching	k20

Vedlegg C Trusseltabellen

39 trusler ble identifisert i risikovurderingen. Truslene er entydig identifisert med en kombinasjon av bokstaver og tall. Bokstavene angir hvilket av sikkerhets-aspektene konfidensialitet (k), kvalitet (q), integritet (i) og tilgjengelighet (t) trusselen er relatert til, og det er en fortløpende nummerering for hver av disse kategoriene.

ID	Trussel / Uønska hendelse	Årsak	Konsekvens	Sannsynlighet	Risiko	Kommentarer (f.eks. forslag til tiltak)
Trusler mot konfidensialitet						
k1	Tilfeldige besøkende hos pasienten – andre i samme rom, *som pasienten vet om* – får kjennskap til sensitiv info om pasienten.	Helsepersonellet vet ikke om andre som er utenfor kameras dekning og sier ting som bare er ment for pasienten	**Liten**	**Stor**	**Lav**	(Det kan være hjemmesykepleier sammen med pasienten.) Rutine: Informere samtaleparten om andre som er til stede i rommet eller som kommer inn i løpet av samtalen.
k2	Tilfeldige besøkende hos pasienten – andre i samme rom, *uten at pasienten vet om det* – får kjennskap til sensitiv info om pasienten.		**Moderat**	**Liten**	**Lav**	
k3	Uvedkommende utenfor huset overhører/ser konsultasjonen	Vinduet står åpent. Skjerm synlig gjennom vindu. Høy lyd.	**Moderat**	**Liten** - men ikke relevant for de to pasientene som er med nå.	**Lav**	Har bevissthet rundt lukking av vinduer og hindrer innsyn til skjermen via vinduer. Evt. headset i stedet for høyttaler.
k4	Andre kommer inn på VK-rom på sykehuset mens VK pågår – og får kjennskap til sensitiv info om en pasient	Skjerm synlig. Høy lyd.	**Liten** – får ikke noe helhetlig info.	**Stor**	**Lav**	Plakat... Eller ”rødt lys” Låse døra! Plassering av skjerm i forhold til dør/vindu. Dempe lyd.

ID	Trussel / Uønska hendelse	Årsak	Konsekvens	Sannsynlighet	Risiko	Kommentarer (f.eks. forslag til tiltak)
k5	Helsepersonell mottar telefon-oppringning mens VK pågår		**Liten** Konsekvens mest for annen pasient, den som telefon-oppringing angår: Pas på VK kan få tausheltsbelagt info om vedk.	**Stor** (Marit enig) Vil skje like ofte som på møter uten VK...	**Lav**	Kan slå av telefon, eller la være å svare. (Vurdere om det er nødvendig å svare.) Kan slå av mikrofon på VK før telefonoppringing besvares.
k6	Oppringing fra andre (VK)-enheter	- fra ”roboter” el.l. på internett, til pasient på internett.	**Liten** - mest et irritasjons-moment	**Svært stor** - basert på hendelser	**Middels**	Autosvar er slått av. Tiltak: Slå av VK-utstyret når det ikke er i bruk (rutine) Finne andre, mer avanserte tiltak?
k6b		- til VK-enhet i helsenettet via ISDN, fra uvedkommende utenfor helsenettet.	**Liten** Oppdages straks	**Liten** - krever en del detaljkunnskap om denne muligheten	**Lav**	Autosvar er slått av.
k7		- bevisst, fra uvedkommende *person* på nettet	**Liten** Oppdages straks	**Liten**	**Lav**	Autosvar er av. I denne tjenesten er det ikke mulighet for flerparts-VK initiert fra pasienten. Hvis en annen enhet forsøker å koble seg opp, også i en pågående VK, kommer det spørsmål på skjermen og man må velge om man vil svare eller avvise. Navn på VK-enhet som ringer inn kommer opp på skjermen, men denne informasjonen kan forfalskes.
k8		- feilringing, fra uvedkommende *person* på nettet	**Liten** Oppdages straks	**Middels**	**Lav**	

ID	Trussel / Uønska hendelse	Årsak	Konsekvens	Sannsynlighet	Risiko	Kommentarer (f.eks. forslag til tiltak)
k9	Uvedkommende på sykehus svarer på VK-oppringing fra pasient (og får dermed vite om at pasienten er i behandling)	Pasienten ringer utenfor avtalt tid	**Liten** Trenger ikke gi noen helse-opplysninger.	**Liten** Rom brukes svært lite av andre, og andre vil neppe svare på en oppringing	**Lav**	Autosvar er slått av, men uvedkommende kan likevel velge å svare. Opplæring/bevisstgjøring til pas (og helsepersonell): Ikke diskutere helseopplysninger med uvedkommende.
k10	Uvedkommende på sykehus ringer opp pasienten	Velger ved en feiltakelse det forhåndslagra nr til pasienten	**Liten** Mest en plage for pasienten. Trenger ikke gi noen helse-opplysninger.	**Middels** Rom brukes lite av andre. Men utstyr kan (generelt) være flyttbart. Feiloppringing skjer ofte, jf. bruk av telefon-liste på mobil.	**Lav**	Pasienten ser at det er en ukjent person, og kan avbryte (legge på), Opplæring/bevisstgjøring til pas. - Pas. har avslått VK-enhet utenom avtalt tidspunkt.
k11	Uvedkommende hjemme hos pasienten (besøkende, andre familiemedlemmer) ringer opp sykehuset	- de bruker det forhåndslagra nr til sykehuset	**Liten** - mest et irritasjons-moment	**Liten** Rom brukes ikke av andre, og andre vil neppe svare?	**Lav**	Ikke autosvar på sykehuset, men uvedkommende kan likevel velge å svare. Opplæring/bevisstgjøring til helsepersonell, og pasient.
k12	Brukerne tror VK er avsluttet, men den er ikke det	Bruker slår bare av skjermen i stedet for å kople ned forbindelsen.	**Moderat** Kan bli sagt ting som ikke var ment for dem i andre enden...	**Middels** - skjer stadig, f.eks. ved VK-undervisning til flere sykehus	**Middels**	Opplæring, bevisstgjøring.
k13	Sykehuset ringer opp ny pasient uten at den forrige er avsluttet.	Gløymt å avslutte etter konsultasjon	**Moderat** Pasientene ser og hører hverandre, men sykehuset vil oppdage det fort og kan avslutte	(Svært) **Liten**	**Lav**	Teknisk mulig, men svært lite sannsynlig da man normalt ser avgløymt studio på skjerm før oppkobling.

ID	Trussel / Uønska hendelse	Årsak	Konsekvens	Sannsynlighet	Risiko	Kommentarer (f.eks. forslag til tiltak)
k14	Bilder fra VK kan legges ut på web – snapshots en gang pr sek (ikke lyd)		**Liten** kun enkeltbilder, ikke lyd	**Liten**	**Lav**	Slå av web-snapshots på VK-enheten (- men kan slås på igjen fra tekniker i helsenettet) Har lagt inn sterke passord for web-aksess til VK-enhet på internett.
k15	Uvedkommende avlytter overføring i nettet	- internett	**Alvorlig**	(Svært) **Liten** - i praksis NULL	**Middels** (NULL)	Kryptert forbindelse, ende til ende
k16		- helsenettet	**Alvorlig**	(Svært) **Liten** - i praksis NULL	**Middels** (NULL)	
k17	Det gjøres utilsiktet opptak av VK-samtalen	- direkte i VK-enheten	**Alvorlig**	(Svært) **Liten** - vanskelig å få til (men vil være enklere hvis det blir lagt inn som rutine)	**Middels**	Ikke mulig med direkte opptak i de VK-enhetene som brukes i denne tjenesten.
k18		Filmes fra annen enhet (f.eks. mobil-telefon eller kamera)	**Alvorlig**	**Liten** - hva skulle motivasjonen være?	**Middels**	Bevisstgjøring til helsepersonell og pasient.
k19		Feilaktig oppringing til opptaksenhet i Helsenettet	**Alvorlig**	**Liten**	**Middels**	Bevisstgjøring, opplæring. Det finnes en recorder i helsenettet som man ved en feiltakelse kan ringe opp – og opptak legges ut på internett. http://tcs.nhn.no
k20	Hacking av VK-enhet via nettet, kan fjernstyre den, avlytte...	Feil/svakheter i programvaren, som blir utnytta	**Alvorlig**	(Svært) **Liten** - men > Null	**Middels**	Det finnes eksempler... Det blei raskt fiksa, og det var en annen type utstyr enn vi har her. Forsøk på innlogging kan ses i logg, det skjer til stadighet på utstyr som er tilknyttet Internett.

ID	Trussel / Uønska hendelse	Årsak	Konsekvens	Sannsynlighet	Risiko	Kommentarer (f.eks. forslag til tiltak)
Trusler mot kvalitet						
q1	Dårlig bildekvalitet (f.eks. så dårlig at display ikke kan leses)	dårlig lys, feil lys, motlys	ganske **Liten** - kan justere underveis	**Middels**	**Lav**	Info/trening/opplæring: Hvordan man håndterer ulike problem som kan oppstå under VK-samtalen. Erfaring Utprøving under installasjon Lede underveis – helsearbeider på sykehus kan styre kamera hos pasienten (zoom, bevege). - Ha rutiner for hva som kan avgjøres via VK (kan variere fra gang til gang utfra kvalitet).
q2		feil justering av skjermen (konfigurering) - men kamera er godt?	**Liten**	**Liten** Som regel bare ved første gangs bruk	**Lav**	
q3		dårlig linje, liten båndbredde, dårlig stabilitet (varierende båndbredde)	**Moderat?** Kan variere fra gang til gang. Hvis det blir for plagsomt (skjer for ofte) kan det bety at man ikke vil benytte tjenesten	**Middels** Erfaring: VK mot den ene pasienten har ofte dårligere kvalitet, mens den andre oftest er ok	**Middels**	Lite å gjøre med, må leve med det... (Kan kanskje hjelpe å avslutte og så kople opp på nytt.) Bytte leverandør
q4	Manglende bilde hos en av partene, bare lyd.	Skjerm ikke slått på, eller kamera ikke slått på i andre enden.	**Liten** - kan justere (rette opp) underveis	**Liten**	**Lav**	Man må ha separat lydanlegg fra skjerm, og man må svare uten å ha bilde (- noe som jo kan skje ved autosvar på). Be om å slå på skjerm/kamera.
q5	Ser ikke den andre parten, person er ikke innenfor bildet	Feil eller manglende styring av kameraet tilpasset behovet til enhver tid.	**Liten** - kan justere underveis	**Middels**	**Lav**	Tiltak: Opplæring

ID	Trussel / Uønska hendelse	Årsak	Konsekvens	Sannsynlighet	Risiko	Kommentarer (f.eks. forslag til tiltak)
q6	Dårlig lydkvalitet	dårlig linje, liten båndbredde, dårlig stabilitet (varierende båndbredde)	**Liten?** Kan variere fra gang til gang. Hvis skjer for ofte, kan det bety at man ikke vil benytte tjenesten. – Men man kan bruke telefon.	**Liten** Lyden mindre påvirka av båndbredde	**Lav**	Kan bruke telefon i tillegg
q7		Feil plassering i forhold til mikrofon (for langt unna)	**Liten** - kan justere underveis	**Stor**	**Lav**	Opplæring – og skru opp lyden på høyttaler
q8		Mikrofon plassert for nær høyttaler	**Liten** - kan justere underveis	**Stor**	**Lav**	Opplæring Det er frittstående mikrofon på begge sider.
q9	Manglende lyd hos en av partene, bare bilde	Mikrofon ikke slått på, eller høyttaler ikke slått på i andre enden	**Liten** - kan justere underveis	**Stor**	**Lav**	Slå på mikrofon... eller høytaler Bruk telefon for å gi beskjed
q10	Enkelt å gjøre feil i oppkopling og avslutning av VK, jf. truslene k9 og k10 over	Brukergrensesnittet for VK kan misforstås	**Liten** Plunder for pasienten	**Liten** Hurtigknapp for oppringing, men kan velge feil nr	**Lav**	Lett å komme tilbake til ”start” hvis man roter seg inn i andre menyer; har gitt opplæring.
Trusler mot integritet *(falsk informasjon)*						
i1	Uvedkommende ringer opp og gir seg ut for å være helsepersonell (jf. truslene k6, k7, k8, k9 foran)		(svært) **Liten** Pasienten kjenner de involverte personene	**Liten**	**Lav**	Hva med bruk av vikarer? Nei... brukes ikke. Vikarer bør introduseres (gjelder begge sider).

ID	Trussel / Uønska hendelse	Årsak	Konsekvens	Sannsynlighet	Risiko	Kommentarer (f.eks. forslag til tiltak)
Trusler mot tilgjengelighet *(kan ikke koble opp)*						
t1	VK-utstyr hos pasienten er blitt stjålet		**Liten** - men tjenesten kan ikke gjennomføres	**Liten**	**Lav**	
t2	VK-utstyr på sykehus er blitt stjålet			**Liten?** Større hvis det hadde vært PC?	**Lav**	Ikke lett omsettelig...
t3	Konfigurasjon er blitt endret slik at VK ikke fungerer lenger	- bevisst handling	**Moderat**? - kan gi dårlig inntrykk av tjenesten at slikt kan skje	(Svært) **Liten** - hva skulle motivasjonen være?	**Lav**	Support er nødvendig. SKIS eller HN IKT?
t4		- ved en feiltakelse		**Liten**? Se trussel q10	**Lav**	
t5	Utstyret blir ødelagt	f.eks. kamera virker ikke...		**Liten** Skjer, men er stabilt	**Lav**	Support er nødvendig. SKIS eller HN IKT?
t6	Nettforbindelse ikke tilgjengelig	Linjebrudd	**Liten** - men tjenesten kan ikke gjennomføres	**Middels**? - kommer an på hvor man bor	**Lav**	Lite å gjøre med, må vente til nettet er oppe igjen...
t7	Fjernkontroll virker ikke	fri for batteri	**Liten** - kan enkelt bytte batteri selv	**Liten** - får kanskje advarsel på forhånd	**Lav**	Opplæring: VK-enhet detekterer det
Andre trusler?						