

Kort sagt om...

Videokonferanse som samhandlingsverktøy

Videokonferanse som velfungerende verktøy setter krav til infrastruktur, lokale tekniske løsninger og rutiner for bruk. Dette faktaarket fokuserer på noen viktige spørsmål man bør ta stilling til ved bruk av videokonferanse.

Videokonferanse defineres her som toveis lyd- og bildeforbindelse. Det finnes både forskjellige typer teknologier og forskjellige modeller innenfor en bestemt teknologi.

Hvilke muligheter gir videokonferanse?

Videokonferanse har et stort potensial for deling av kunnskap og gir nye muligheter for kommunikasjon. Uavhengig av avstand kan man for eksempel:

- Spre kunnskap og foreta opplæring nasjonalt og internasjonalt
- Opprette kommunikasjonskanal mellom alle profesjoner og nivåer i helsevesenet
- Gå fjernvisitt hos pasient
- Avholde møter
- Ha ad hoc diskusjoner mellom aktører i helsevesenet
- Ha møte mellom helse- og sosialarbeider på den ene siden, og pasient og/eller pårørende på den andre siden



Samhandling via videokonferanse.

Foto: Jan Fredrik Frantzen, Nasjonalt senter for telemedisin

Hvilke krav stilles til videokonferanse?

Bruk av videokonferanse som samhandlingsverktøy må planlegges nøye. For å sikre god kvalitet på tjenesten, er det viktig at følgende er på plass:

- Infrastruktur
- Tekniske løsninger og sikkerhet
- Organisatoriske tiltak

Teknisk infrastruktur

Videokonferanse stiller store krav til infrastruktur for å fungere godt. I dag er det vanlig å bruke datalinjer som kommunikasjonskanal istedenfor ISDN telefonlinjer som var mer vanlig før. Det må til enhver tid vurderes om den forbindelsen man har tenkt å bruke har den kvalitet, sikkerhet og konfigurering som kreves:

Hastighet

Minst 2 Mbps hastighet begge veier til og fra nettet er en god forbindelse som passer de fleste. Bruker man en asynkron forbindelse (f.eks. ADSL) bør man sjekke at hastigheten er stor nok begge veier.

Konfigurering

Brannmur og switcher må konfigureres riktig. Mange porter må være åpne for å få til en vellykket videokonferanse. I lokale nett kan sikkerhetspolicy gjøre at det kan være problematisk å sette inn videokonferanse i samme nettet som datamaskinene. Et eget dedikert nett til videokonferanse er ofte den enkleste løsningen.

Kvalitet og stabilitet

Stabile linjer der stor båndbredde er tilgjengelig til enhver tid vil sikre god kvalitet på videokonferansene. Ved videokonferanse sendes data i sanntid og tapte data vil ikke sendes på nytt. Tap av data vil derfor forringe kvaliteten og kan føre til brudd og problemer med oppkoblingen. Dedicerte nett til videokonferanse og noe overdimensjonering av båndbredde kan være løsningen hvis man har problemer med stabilitet.

Videokonferanse over Internett

Har man videokonferanse over Internett vil man som regel ikke kunne garantere kvaliteten på forbindelsen. Internett er dynamisk og redundant i sin struktur, og det kan være forskjell på forbindelsen fra en dag til neste selv om man kobler opp til samme lokasjon. Kun statistiske data eller erfaring kan fortelle om hva man kan forvente ved oppkobling over Internett.

Testing av en Internettforbindelse dager eller timer i forveien har derfor begrenset verdi. Man får bare et øyeblikksbilde av forbindelsen. Flere oppkoblinger over tid vil gi et mer korrekt bilde av hva man kan forvente.

Norsk Helsenett (NHN)

Norsk Helsenett jobber for å kunne levere et kvalitets-sikret videokonferansenett til helsesektoren i Norge. De vil derfor være en naturlig aktør å kontakte i forbindelse med etablering av videokonferanse i helsevesenet. Se www.nhn.no for kontaktinformasjon.

>>



Tekniske løsninger og sikkerhet

Hjemme kan man ha videokonferanse fra sin PC med for eksempel programmene MS Messenger eller Skype og et web-kamera. I helsevesenet er imidlertid ikke dette regnet som en god løsning, av flere grunner:

Sikkerhet

Helseopplysninger er sensitive. Bare rette vedkommende skal gis kjennskap til denne informasjonen. Dette innebærer at helseopplysninger som formidles elektronisk over et nettverk må krypteres, også om de formidles via videokonferanse.

Det er ikke forsvarlig å bruke en privat PC tilknyttet Internett for å overføre pasientsensitiv informasjon. En PC kan få virus eller annen ondsinnet programvare, slik at sensitive data kommer på avveie eller blir lagret uten brukers viten. Noen typer ondsinnet programvare kan overvåke PC-en og videreformidle alt brukeren gjør på PC-en, inkludert det skjermbildene viser, til uvedkommende. Generelle svakheter og angrep mot PC-er på nettet gjelder også for bruken av web-kamera og video. Det oppdages stadig nye svakheter som må repareres. Det er svært viktig å være påpasselig med beskyttelsestiltak, sikkerhetsoppdateringer, osv. Privat hjemme-PC anses derfor, på et generelt grunnlag, ikke å ha god nok sikkerhet til å kunne benyttes til formidling av helseopplysninger.

Stabilitet

Programmene MS Messenger og Skype er avhengig av en egen server for å finne adressen til andre brukere. Fordi man i dag er avhengig av at denne tjenesten driftes av andre selskaper, som oftest utenfor Norge, vil det være uvisst hvilken support og stabilitet dette gir. Andre programmer på en PC kan påvirke kvaliteten på kommunikasjonen. Det kan være komplisert å finne ut om det er en feil med PC eller feil i videokonferansen som er problemet.

Kompatibilitet

Programmene MS Messenger og Skype er ikke kompatible med andre større profesjonelle videokonferanseløsninger. Det vil derfor ikke være mulig å snakke fra for eksempel Skype til en Sony, Polycom, Tandberg eller Aethra videokonferansenhet. PC-software som er kompatibel med profesjonelle videokonferansesystemer er å få kjøpt, men man vil fortsatt måtte ta hensyn til PC-sikkerheten.

Den vanligste løsningen i helsevesenet i dag er derfor å ha eget/dedikert utstyr som bruker kommunikasjonsprotokollen H.323. Moderne løsninger har innebygd mulighet til å kryptere samtalen.

Disse systemene finnes i et vidt spekter fra små personlige løsninger til større anlegg, sistnevnte for eksempel innebygget i et auditorium.

Andre sikkerhetstrusler

Kommunikasjonen mellom moderne videokonferansesystemer kan krypteres. Den blir da svært vanskelig å avlytte.

Det finnes likevel andre sikkerhetstrusler, men disse kan i stor grad forhindres ved gode rutiner:

- Krypteringen kan bli slått av automatisk, bl.a. dersom mottaker ikke støtter krypteringen. Brukeren må derfor forsikre seg om at krypteringen er på. I noen systemer er det slik at innkommende telefonsamtaler i videokonferansen medfører at krypteringen slås av uten at det gis eksplisitt beskjed om dette. Symbolet for kryptering endrer seg imidlertid.
- Det kan være personer utenfor kameras synsfelt som man ikke vet om.
- Det kan være opptaksutstyr koblet til videokonferansenheten (VHS, DVD opptaker) som lagrer konferansen.
- Utstyr kan være satt i autosvarmodus, dvs. at man kan få satt opp en forbindelse mot en enhet uten at noen på mottakersiden aktivt aksepterer at forbindelsen settes opp.
- Kamera fungerer like godt selv om skjermen er avslått. I forbindelse med autosvarmodus kan dette medføre at det kan sendes bilde og/eller lyd fra et lokalt der videokonferanseutstyr er installert, uten at de som er til stede er klar over det.

Viktige organisatoriske tiltak for en velfungerende videokonferansetjeneste

Man skal ikke gjøre seg avhengig av videokonferanse i livsviktige eller tidskritiske situasjoner. Videokonferanse har for mange ukjente faktorer til at man kan garantere en 100 % stabil og sikker tjeneste.

Bruk av videokonferanse innenfor en organisasjon vil, over tid, kun fungere godt hvis følgende er på plass:

- Brukere som er motivert for å bruke videokonferanse, både på sender- og mottakersiden.
- Lokal teknisk kompetanse på videokonferanse og rutiner for support.
- Studioansvarlig som har ansvaret for å holde utstyret operativt og som kan veilede nye brukere.
- Klare rutiner for booking og bruk av utstyr og rom.
- Integrasjon av videokonferanse i daglige arbeidsrutiner.

Kontaktpersoner NST:

Datasikkerhet:

Eva Henriksen
eva.henriksen@telemed.no
Tlf: +47 957 31 836

Videokonferanseutstyr:

Stig Karoliussen
stig.karoliussen@telemed.no
Tlf: +47 415 15 090

Eva Skipenes
eva.skipenes@telemed.no
Tlf: +47 911 77 515

Jan Hugo Olsen
jan.hugo.olsen@telemed.no
Tlf: +47 415 15 095

Se www.telemed.no/faktaark for andre faktaark i serien. Dette faktaarket ble sist revidert i juli 2008.

