

 NORMEN Norm for informasjonssikkerhet www.normen.no	Utgitt med støtte av: 
<h2>Videokonsultasjon</h2>	Støttedokument Faktaark nr. 54 Versjon: 2.0 Dato: 16.04.2020

Formål	Gi virksomheten oversikt over hvilke krav som skal ivaretas ved etablering og bruk av videokonsultasjon.		
Ansvar	Virksomhetens ledelse er ansvarlig for at bruk av videokonsultasjon ivaretar pasientrettigheter- og sikkerhet, taushetsplikt, personvern og gir nødvendig informasjonssikkerhet i hele løsningen.		
Gjennomføring	Ved planlegging av bruk av videokonsultasjon skal virksomheten dokumentere at nødvendige sikkerhetsløsninger er etablert. Benyttes ekstern leverandør / databehandler for hele eller deler av løsningen må denne dokumentere sin del av løsningen og det skal inngås databehandleravtale.		
Omfang og avgrensning	<p>Gjelder bruk av videokonsultasjon mellom helsepersonell og pasient ved ytelse av helsehjelp og mellom helsepersonell uten at pasient deltar. Faktaarket kan benyttes internt i virksomheten og mot leverandør.</p> <p>Faktaarket omfatter ikke lagring av videokonsultasjoner.</p> <p>Før videokonsultasjon kan tas i bruk må kliniske forhold rundt ytelse av forsvarlig helsehjelp vurderes. I forkant av en videokonsultasjon må medisinskfaglig ansvarlig gjøre en vurdering om det er faglig forsvarlig å gjennomføre konsultasjonen som videokonsultasjon. Faktaarket omtaler ikke disse momentene.</p> <p>Faktaarket omfatter planlagte videokonsultasjoner. I akutsituasjoner kan videokonsultasjoner fra en nødrettsbetraktning av og til være nødvendig for å gi pasienten trygg og rask behandling. At utradisjonelle tiltak, som video, benyttes i kritiske situasjoner kan forsvares i enkelttilfeller, men når det kan ikke gå over i en systematisk praksis. Faktaarket omtaler ikke dette.¹</p>		
Målgruppe Dette faktaarket er spesielt relevant for:	<input checked="" type="checkbox"/> Virksomhetens leder/ledelse <input type="checkbox"/> Forskningsansvarlig <input type="checkbox"/> Prosjektleder forskning <input checked="" type="checkbox"/> Sikkerhetsleder	<input checked="" type="checkbox"/> Ansatt / medarbeider <input type="checkbox"/> Forsker <input checked="" type="checkbox"/> Personvernombud	<input checked="" type="checkbox"/> IKT-ansvarlig <input checked="" type="checkbox"/> Databehandler <input checked="" type="checkbox"/> Leverandør
Referanser	<ul style="list-style-type: none"> Personvern og informasjonssikkerhet i kontakten med pasient/bruker, En veileder i bruk av portalløsninger, SMS og e-post Video-, lyd- og bildeopptak i helse- og omsorgssektoren - en veileder. Veilederen omtaler bl.a. lagring av videoopptak Faktaark 10 – Bruk av databehandler (ekstern driftsenhet) Faktaark 14 – Tilgangsstyring Faktaark 15 – Logging og oppfølging av logger Faktaark 19 – Tiltak for å hindre ondsinnet programvare Faktaark 47 – Autorisasjonsregister Faktaark 49 – Krav ved bruk av PKI ved ekstern kommunikasjon Vedlegg "Oversikt over Normens krav" 		

¹ Se om dette i [Rundskriv om informasjonshåndtering i spesialisthelsetjenesten](#)

Eksterne referanser	Direktoratet for e-helses sider for video: <ul style="list-style-type: none"> • https://ehelse.no/aktuelt/korona-slik-kommer-du-i-gang-med-videokonsultasjon • https://ehelse.no/aktuelt/praktiske-rad-til-helsepersonell-om-god-bruk-av-videokonsultasjon Kvikkguide til implementering av videokommunikasjon - Nasjonalt velferdsteknologiprogram, publiseres 17.4.2020
----------------------------	---

Med ”**videokonsultasjon**” menes i dette faktaarket ytelse av helsehjelp med videooverføring hvor pasienten enten er til stede i videokonsultasjon eller omtales med identifiserende opplysninger.

Videokonsultasjon kan gjennomføres ved at pasienten bruker virksomhetens utstyr eller sitt eget private utstyr. Risikoene og tiltakene blir da forskjellige. Dette er viktige momenter i vurderingen, bl.a. med tanke på sikring og autentisering av utstyret.

I en videokonsultasjon kan pasienten eller helsepersonellet være kjent fra før eller hen kan være ukjent. Dette er et viktig moment i vurderingen, bl.a. med tanke på autentisering og informasjon.

Eksempler på videokonsultasjon

- planlagte møter mellom pasient og helsepersonell
- tverrfaglige møter uten at pasienten er til stede
- pasienten er hos (sammen med) annet helsepersonell: fastlege, fysioterapeut, hjemmesykepleier, i annen institusjon, etc.
- flerpartskonsultasjon med grupper for terapi, trening e.l. med en behandler og flere pasienter til stede
- kommunikasjon/ konsultasjon/oppfølging mellom pleie- og omsorgstjenesten i kommunen og pasient/bruker i eget hjem
- flerpartskonsultasjon mellom for eksempel spesialist på sykehus, fastlege og pasient hjemme
- tolketjeneste hvor pasient, helsepersonell og tolk deltar
- opplæring av pasient
- legevisitt
- sanntidsoverføring fra skadested (for eksempel fra ambulanse) til helsepersonell ved sykehus

Normens krav til informasjonssikkerhet ved videokonsultasjon med pasient/bruker

Tabellen nedenfor viser noen av Normens krav og mulig løsning for hvordan kravene for eksemplene ovenfor kan ivaretas.

Virksomheten er ansvarlig for (krav fra Normen)	Utdypning av krav og mulige løsninger
Sikre lovlig behandling Se mer i Normen kap 4.1	Personopplysninger kan bare behandles når lovgivningen tillater det. All behandling av personopplysninger skal ha et lovlig behandlingsgrunnlag. Samtykke er rettsgrunnlaget for ytelse av helse- og omsorgstjenester. Ved videokonsultasjon vil det ofte være et implisitt samtykke at pasienten ønsker å få helsehjelp da hun tar i bruk løsningen og deltar i konsultasjonen. Helselovgivningen gir behandlingsgrunnlag for behandling av de opplysningene som er relevant og nødvendig for ytelse av helsehjelp

Virksomheten er ansvarlig for (krav fra Normen)	Utdypning av krav og mulige løsninger
	<p>via videokonsultasjon. Det er derfor ikke nødvendig med et eget samtykke for behandling av personopplysninger når videokonsultasjon brukes til å yte helsehjelp.</p> <p>Bruk av videokonsultasjon for andre formål enn å yte helsehjelp, f.eks. forskning, kan ha andre behandlingsgrunnlag.</p>
<p>Informasjon til pasient om bruk av videokonsultasjon der pasient er involvert</p> <p>Se mer i Normen kap 4.2.2</p>	<ol style="list-style-type: none"> 1. Før videokonsultasjon starter skal pasienten få informasjon om videokonsultasjon og behandling av helse- og personopplysninger i videokonsultasjon. 2. Informasjon kan gis muntlig eller skriftlig <p>På ehelse.no finner du mer om informasjon til pasient, https://ehelse.no/aktuelt/korona-slik-kommer-du-i-gang-med-videokonsultasjon#Informasjon%20til%20pasienten</p>
<p>Entydig identifisering av pasienten/brukeren/ helsepersonell (Autentisering)</p> <p>Se mer i Normen kap 5.2</p>	<ol style="list-style-type: none"> 1. Det skal gjennomføres risikovurdering som blant annet viser at pasienten/brukeren identifiseres entydig 2. Ved første gangs videokonsultasjon med ukjent pasient skal pasient/innbyggeren entydig identifiseres <ul style="list-style-type: none"> • Et løsningsalternativ er bruk av personlige kvalifiserte sertifikater med for eksempel pålogging tilsvarende Bank-ID eller mekanismer i ID-porten. Bruk av personlig kvalifisert sertifikat sikrer at autentiseringskriterier tildeles på en betryggende måte • Dette kan også ivaretas ved at deltagerne viser gyldig legitimasjon 3. Er pasienten kjent for helsepersonellet, vil video av pasienten kunne oppfylle kravet om entydig identifisering. Risikovurderingen skal dokumentere dette 4. Helsepersonell skal autentiseres på en sikker måte. Risikovurderingen skal fastsette hva som er sikker måte. 5. I tilfeller der det er umulig å sikre entydig identifikasjon, f.eks. ved kognitiv svikt hos pasient, kan et alternativ være å sikre entydig identifisering av utstyret.
<p>Entydig identifisering av utstyr levert av virksomheten (Autentisering)</p> <p>Se mer i Normen kap 5.2</p>	<ol style="list-style-type: none"> 1. For utstyr levert av virksomheten er utgangspunktet at løsningene er installert og konfigurert med faste kommunikasjonspunkter som kan være behandlingsrom eller hjemmet til pasienten. 2. Om risikovurderingen konkluderer med at det er behov for autentisering av utstyret på en sikker måte, kan det gjøres med for eksempel: <ul style="list-style-type: none"> • MAC-adresse, IMEI-nummer eller bruk av offentlig og privat nøkler som genereres på utstyret. Den offentlige nøkkelen må deles med tjenesten ved oppsett. Nøkkelparet er ulikt for hver løsning i virksomheten. • Nettverksautentisering basert på for eksempel sertifikater 3. Tildeling av slike autentiseringskriterier skal gjøres på en betryggende måte som vil si etter fastsatte prosedyrer
<p>Kryptering av kommunikasjon</p> <p>(Se mer i Normen kap 5.3.5)</p>	<ol style="list-style-type: none"> 1. All kommunikasjon utenfor virksomhetens kontroll, skal krypteres² 2. All kryptering og dekryptering mellom kommunikasjonspunkter i infrastrukturen skal gjøres i godkjent utstyr virksomheten har kontroll med. Hvis det benyttes leverandør til dette skal det sikres at databehandleravtalen dekker leverandørens behandling av personopplysninger.

²Se for eksempel dokumentet «NSM Cryptographic Requirements Version 3.1» og Level Moderate

Virksomheten er ansvarlig for (krav fra Normen)	Utdypning av krav og mulige løsninger
Logging av hvem som har hatt tilgang til eller fått utlevert helseopplysninger (Se mer i Normen kap 5.4.4)	<ol style="list-style-type: none"> 1. Videokonsultasjon skal følge samme dokumentasjonsplikt som ordinære konsultasjoner 2. Videokonsultasjon mellom pasient og helsepersonell skal logges. 3. Hvis videokonsultasjon ikke har funksjonalitet for automatisert logg, skal helsepersonellet manuelt logge at det er gjennomført videokonsultasjon med pasient, ved nedtegnelse i pasientens journal.
Ivareta taushetsplikten (Se mer i Normen kap 4.2.1)	<ol style="list-style-type: none"> 1. På samme måte som ved fysisk oppmøte, vil helsepersonellovens regler om taushetsplikt være styrende for selve samtalen og behandling av informasjon som fremkommer 2. Virksomheten må ha rutiner som ivaretar taushetsplikten ved videokonsultasjon. <ul style="list-style-type: none"> • Hvis man f.eks. skal utføre en videokonsultasjon hjemmefra må det vurderes hvordan man skal overholde taushetsplikten. Eks. sitte i et rom som er avskjermet fra innsyn fra familie/tredjeparter, skjerming av lyd osv. 3. Virksomheten må ha en teknisk løsning og/eller rutine som sikrer at kun godkjente deltagere deltar i videokonsultasjon 4. Det må være synlig hvem som til enhver tid deltar i samtalen 5. Deltar flere pasienter skal alle pasientene få informasjon om dette
Lagring av samtaler og data om samtaler, samt deling av dette	<ol style="list-style-type: none"> 1. Innhold fra samtaler skal ikke lagres i videoløsningen, med mindre videoløsningen er/ er en del av et behandlingsrettet helseregister 2. Virksomheten må sikre at leverandøren av videoløsningen ikke deler data om samtaler (samtaleparter, varighet osv.) med tredjeparter
Personvernrettigheter (Se mer i Normen kap 4.2)	<ol style="list-style-type: none"> 1. Virksomheten skal sikre at videoløsningen ivaretar partenes personvernrettigheter på en enkel og god måte. 2. Løsningen skal ikke forutsette at det gis tilgang til andres personopplysninger fra samtalepartenes utstyr - f.eks. dersom man får full tilgang til kontakter i hverandres kontaktlister
Innebygget personvern	<ol style="list-style-type: none"> 1. Videokonsultasjon-løsningen skal oppfylle personvernforordningens krav til innebygd personvern. 2. I de tilfellene det krever en spesiell konfigurering for å ivareta sikkerhet, personvern og taushetsplikten på best mulig måte må det tydelig fremgå, både til helsepersonell og pasient, hvilke innstillinger som skal velges. <ul style="list-style-type: none"> • Leverandør bør kunne bistå med dette.

Risikovurdering

Virksomheten skal gjennomføre og dokumentere risikovurdering av løsningen før den tas i bruk for å påse at sikkerhetstiltakene er egnet og ivaretar Normens krav til personvern og informasjonssikkerhet. Se Faktaark 07 – Risikovurdering på www.normen.no.

Benyttes databehandler kan det være en praktisk tilnærming at databehandler vurderer teknisk løsning sammen med virksomheten og virksomheten vurderer den funksjonelle løsningen.

Personvernkonsekvensvurdering

Virksomheten skal vurdere konsekvenser for personvernet til de som er involvert i videokonsultasjonen. Hvis det er sannsynlig at en behandling medfører høy risiko for de

involverte, skal virksomheten gjennomføre en mer grundig personvernkonsekvensvurdering, også kalt DPIA etter personvernforordningens artikkel 35. Vurderingen skal dokumenteres. Les mer om høy risiko i Normen kapittel 3.5.1.

Leverandøren av løsningen kan bistå i vurderingen.

Eksempel på scenarier som kan brukes i risikovurdering og personvernkonsekvensvurdering

1. Uautorisert utlevering av helseopplysninger:
 - a. Pasient er ikke alene ved bruk av videokonsultasjon (påørende, hjemmesykepleien, NAV, andre), med mindre pasienten selv ønsker det
 - b. Flere helsepersonell er til stede, men pasient vet ikke det / ser ikke det
 - c. Uvedkommende utenfor rommet ser eller overhører konsultasjonen
 - d. Uvedkommende kommer inn i rommet under konsultasjonen
 - e. Pasient tror videokonsultasjon er avsluttet/nedkoplet, noe den ikke er
2. Videokonsultasjon tas opp og spres til utenforstående
3. Uønsket spredning av videokonsultasjon pga ondsinnet programvare (virus o.l.) på pasientens private PC/nettbrett/mobiltelefon
4. Kommunikasjonen i videokonsultasjon avlyttes
5. Krypteringen brytes underveis i utstyr virksomheten ikke har kontroll med
6. En av partene ringer opp feil utstyr/enhet og det utveksles personopplysninger
7. Feiltolkning av innhold i videokonsultasjon. Dårlig linje, liten båndbredde, varierende stabilitet i Internett, dårlig bilde, dårlig eller manglende lyd
8. videokonsultasjon kan ikke startes (kobles opp) som planlagt. Feil på utstyr hos en av partene. Feil i datanettet. Utstyr er fjernet
9. Stans i videokonsultasjon under bruk
10. Autentiseringskriteria tildeles uautoriserte
11. Pasient er ikke entydig autentisert
12. Helsepersonell er ikke autentisert på en sikker måte
13. Uautoriserte kobler seg til virtuelle møterom
14. Medarbeidere hos leverandøren får tilgang til helse- og personopplysninger.
15. Leverandøren mellomlagrer video med lyd i sin løsning uten av Normens krav er ivarettatt
16. Leverandøren er plassert i EU/EØS
17. Leverandøren er plassert utenfor EU/EØS
18. Skytjenesteleverandør oppfyller ikke lovbestemte krav og Normens krav
19. Mangelfull plan ved avslutning av skytjeneste
20. Ved skjermdeling viser helsepersonell ved feiltagelse sensitiv informasjon om annen pasient
21. Pasient tar opp samtalen uten tillatelse

Rutiner og opplæring

Det skal etableres rutiner for bruk og drift av videokonsultasjon. Hvilke rutiner som er nødvendig tilpasses løsningen som tas i bruk. Eksempler:

Rutine	Forslag til innhold
Tilgangsstyring	<ul style="list-style-type: none">• Endre tilganger• Avslutning av tilganger
Autorisering og autentisering av pasient	<ul style="list-style-type: none">• Beskrivelse av hvordan pasient autoriseres• Beskrivelse av hvordan pasient autentiseres for å sikre entydig identifisering
Autorisering og autentisering av helsepersonell.	<ul style="list-style-type: none">• Autorisere helsepersonell til tjenstlig behov• Beskrivelse av hvordan helsepersonell autoriseres• Beskrivelse av hvordan helsepersonell autentiseres på en sikker

Rutine	Forslag til innhold
	måte
Kryptering av kommunikasjon	<ul style="list-style-type: none"> Jevnlig kontroll at kommunikasjon er kryptert
Sikre at kun godkjente deltagere deltar i videokonsultasjon for å ivareta taushetsplikten	<ul style="list-style-type: none"> Sikre at kun helsepersonell med tjenstlig behov deltar i videokonsultasjon Informere pasienten når flere pasienter eller helsepersonell skal delta i videokonsultasjon Hvordan håndtere at pasienten lar andre være tilhører/tilstede i samtalen med tanke på taushetsplikt.
Periodisk kontroll av tildelte rettigheter	<ul style="list-style-type: none"> Kontroll av tildelte rettigheter for helsepersonell Kontroll av tildelte rettigheter for administratorbruker
Journalføring av helse- og personopplysninger	<ul style="list-style-type: none"> Ansvar for journalføring Hva som skal journalføres Tidspunkt for journalføring
Bruk av helsepersonellens private utstyr ved videokonsultasjon (mobiltelefon, nettbrett, PC)	<ul style="list-style-type: none"> Minimumskrav til utstyret Sikring av helse- og personopplysninger på utstyret Hvordan videokonsultasjon-løsningen implisitt ivaretar kravet til sikring av helse- og personopplysninger
Informasjon og opplæring av helsepersonell	<ul style="list-style-type: none"> Temaer i opplæringen; bruk av løsningen, tid og sted for videokonsultasjon, informasjonssikkerhet og personvern Tidspunkt for opplæring
Informasjon til pasient	<ul style="list-style-type: none"> Temaer i informasjon; bruk av løsningen, tid og sted for videokonsultasjon og personvern
Andre rutiner som må vurderes dersom løsningen krever det	<p>Administratortilganger</p> <ul style="list-style-type: none"> Administratorbrukere som skal etableres Systembrukere som skal etableres Krav til personlig brukerkonto for administratortilgang Autorisering av administratortilgang <p>Autentisering av administratortilgang</p> <p>Autorisering og autentisering av helsepersonell</p> <ul style="list-style-type: none"> Ulike ansettelsesforhold skal identifiseres Tidsbegrensning av autorisasjonen <p>Registrering av tildelt autorisasjon i autorisasjonsregister</p>

Bruk av tolk ved videokonsultasjon

Bruk av tolk kan løses både ved at tolken deltar fysisk sammen med helsepersonell eller som egen deltager i videokonsultasjon. Ved egen deltagelse gjelder kravene til autorisering, autentisering og kryptering. Se omtale av kravene ovenfor.

Bruk av databehandler

Benyttes det en tjeneste som leveres av en ekstern driftsleverandør skal det opprettes databehandleravtale mellom virksomheten og databehandler. Dette gjelder alle tjenester hvor det behandles helse- og personopplysninger.

Se avtaleeksempel i Faktaark 10 – Bruk av databehandler (ekstern driftsleverandør) (på www.normen.no).

Se også Vedlegg til Normen "Oversikt over Normens krav" med bl.a. følgende krav databehandler skal ivareta:

- At løsningen oppfyller lovbestemte krav og kravene i Normen
- Taushetsplikt for egne medarbeidere
- Internkontroll, sikkerhetsrevisjoner og avviksbehandling

- Ved terminering skal det foreligge en signert erklæring fra leverandøren om at alle data tilhørende virksomheten er tilbakelevert eller slettet til avtalt tid

Sjekkliste med krav som virksomheten (eller databehandler) må ivareta i løsningen:

I tillegg til faktaarket er det publisert en sjekkliste som virksomheten kan benytte ved planlegging og bruk av videokonsultasjon. [Se Faktaark 54 – Videokonsultasjon – sjekkliste.](#)