OVERORDNET RISIKOVURDERING KNYTTET TIL BRUK AV VIDEOKONSULTASJON

Koronasituasjonen

16.04.2020

Norsk Helsenett SF

norskhelsenett

1 BAKGRUNN

På grunn av situasjonen rundt korona-pandemien har fastleger behov for effektiv digital avstandsoppfølgning av innbygger/pasienter, for eksempel ved spørsmål, diagnostisering og oppfølgning i koronaepidemien. Med bakgrunn i dette har HOD gitt Direktoratet for e-helse i oppdrag å se på hvilke muligheter som finnes for å gjennomføre videokonsultasjoner som samtidig ivaretar krav til sikkerhet og personvern.

Det er etablert noen minimumskrav til sikkerhet, og risikovurderingen tar utgangspunkt i disse.

Vurderingene og kravene som er satt er å anse som et midlertidig tiltak for å løse et prekært behov. Det kan være risikoer i bruk av video som ikke er adressert som følger av dette.

Det er ditt ansvar som dataansvarlig (databehandler) å sørge for å utarbeide en tilstrekkelig risikovurdering som hensyntar virksomhetens forhold knyttet til bruk av video i pasientbehandlingen.

2 BESKRIVELSE AV INFORMASJONENS OG/ELLER FUNKSJONENS SIKKERHETSBEHOV

Videokonsultasjon åpner for direktedialog mellom pasient og behandler gjennom å ta i bruk ulike videotjenester. I en slik løsning vil det utveksles personopplysninger, også særlig kategori personopplysninger (helseopplysninger). Det er derfor svært viktig at de digitale videotjenestene ivaretar behovet for å holde informasjon og videostrømmen konfidensiell.

For å levere en god videokonsultasjonsopplevelse til pasient er det dessuten viktig med god nettverksforbindelse for å kunne levere akseptabel kvalitet på lyd og bilde.

Det finnes alternativer til videokonsultasjon, f. eks. telefoni og fysisk oppmøte, men det antas at man i den fasen man er i dag vil bli mer og mer avhengig av at video er tilgjengelig.

3 BESKRIVELSE AV AKTØRER OG INFORMASJONSFLYT

Videokonsultasjon foregår mellom pasient og behandler som en direktedialog, og det kan i enkelte tilfeller være behov for å ha med tolk.

Leverandør av tjenesten vil også være en aktør i informasjonsflyten, men ved å etablere definerte minimumskrav vil ikke leverandøren ha tilgang til informasjonen som deles gjennom video.

4 MINIMUMSKRAV TIL VIDEOTJENESTENE

Alle virksomheter er pliktige til å etablere egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet for å håndtere risiko på en tilfredsstillende måte. I slike vurderinger er det alltid noen sikkerhetskriterier som er viktigere enn andre for å kunne oppnå et akseptabelt nivå av sikkerhet. I situasjoner som Norge og verden nå befinner seg i, må risiko for smitte vurderes opp mot krav til bl.a. informasjonssikkerhet. Det er allerede meldt om ondsinnede aktører som utnytter pandemisituasjonen vi står ovenfor gjennom f. eks. phisingangrep, så hensynet til informasjonssikkerhet må tas med som et viktig kriteria for valg av tiltak.

For å forenkle vurdering av ulike videotjenester har det blitt utarbeidet et sett med minimumskrav som må være oppfylt før en tjeneste tas i bruk. Disse minimumskravene er satt for å minske de eventuelle negative konsekvensene en slik tjeneste kan ha for personvernet til behandler og pasient.

Kravene vil også kunne bistå i å forenkle vurderingen av de enkelte leverandørene av tjenestene som velges.

4.1 FØLGENDE MINIMUMSKRAV ER DEFINERT FOR VIDEOTJENESTENE:

4.1.1 Kryptering

Kryptering er et absolutt krav i en videokonsultasjonsløsning. Normen krever at tekniske tiltak skal etableres slik at all kommunikasjon av helse- og personopplysninger utenfor virksomhetens kontroll krypteres. Krave til kryptering trekkes også fram som et egnet tiltak i personvernforordningen.

Det anbefales å velge løsninger som tilbyr ende-til-ende kryptering, og I hht Normen kap 5.3.5 kan kontroll med kryptering og dekryptering mellom kommunikasjonspunkter i infrastrukturen ivaretas gjennom avtale.

4.1.2 Autentisering

Autentisering av pasientene er et viktig krav ved etablering av videokonsultasjonsløsning. Dette gjelder særlig der pasient er ukjent for helsepersonellet. I mange tilfeller vil pasienten være kjent for det helsepersonellet som gjennomfører videokonsultasjonen, men det vil være situasjoner der pasienten er ukjent. I mange løsninger kan pasienten autentisere seg ved bruk av ID-porten og dette er å foretrekke, og/eller der det er helsepersonell tar utgangspunkt i listesystemet og personnummer til pasient og sender påloggingslenke til pasient. Der løsningen ikke støtter slik funksjonalitet, eller hvor det er rutine hvor helsepersonell sender ut påloggingslenke, kan det iverksettes enklere organisatoriske tiltak hvor ukjent pasient bes identifisere seg med førerkort/bankkort eller lignende når videokonsultasjonen er startet.

Andre organisatoriske tiltak kan være å sende lenke til pasient via kommunikasjonskanaler som e-post. Når det i tillegg er etablert ende-til-ende kryptering betyr det at dersom en uautorisert aktør stjeler lenke, vil ikke vedkommende kunne nyttiggjøre seg av lenken.

4.1.3 Synlighet på hvem som deltar

Det skal være lett synlig hvem som deltar på video. Spesielt for videoløsninger der det er muligheter for flerpart må det tydelig fremgå hvem som deltar i videosamtalen.

4.1.4 Personvernforordningen

Leverandør av videotjenesten skal kunne forplikte seg til å etterleve kravene i personvernforordningen (GDPR). Det må utarbeides en personvernkonsekvensutredning for bruken av video.

4.1.5 Personvernrettigheter

Videoløsningen skal ivareta partenes personvernrettigheter på en enkel og god måte, og tjenesten skal ivareta krav til innebygget personvern.

4.1.6 Hindre deling av personopplysninger

Personopplysninger som oppgis skal ikke brukes til andre formål enn videotjenesten. Dette betyr at det ikke skal kunne deles personopplysninger med andre deler av leverandørens løsninger eller eksterne parter.

4.1.7 Virksomhetens krav til rutiner

Virksomheten som tar i bruk videoløsningen skal sørge for å ha på plass gode rutiner for bruk av videoløsningen og informasjon til pasient/ bruker.

4.1.8 Ingen lagring av innholdet i videosamtalene

Det skal ikke lagres data fra videosamtalene hverken hos behandler, pasient eller leverandør av videotjenesten.

4.1.9 Taushetsplikt

Tasushetsplikten forutsettes ivaretatt også ved bruk av videoløsninger.

5 ØVRIGE STØTTEDOKUMENTER

5.1 PERSONVERNKONSEKVENSVURDERING

Disse vurderingene vil ta utgangspunkt i minimumskriteriene som nevnt i denne risikovurderingen, og gjøres tilgjengelig på www.ehelse.no etter hvert som ulike løsninger blir vurdert

5.2 TJENESTEBESKRIVELSER

For å sikre at minimumskravene oppfylles ved oppsett av nye tjenester vil det utarbeides detaljerte beskrivelser av hvordan tjenesten skal konfigureres. Dette går for de fleste tjenestene ut på å fjerne mye av funksjonaliteten som ligger i dem, men åpne for video.

Veiledninger vil gjøres tilgjengelig på www.ehelse.no etter hvert som ulike løsninger blir vurdert.

6 AVGRENSNING AV RISIKOVURDERING

Risikovurderingen er generell, og omhandler bruk av video som imøtekommer minimumskravene gjengitt i denne risikovurderingen. Dataansvarlig er selv ansvarlig for å lage en risikovurdering som tar hensyn til de virksomhetsspesifikke forholdene knyttet til bruk av video i pasientbehandlingen. Dette kan som et eksempel være knyttet til interne rutiner for bruk av tjenesten da det her vil være en rekke manuelle tiltak som må på plass knyttet til identifisering, logging og journalføring og lignende.

7 IDENTIFISERTE TRUSLER

Nedenfor stiller vi opp en vurdering som du som behandlingsansvarlig kan ta utgangspunkt i når du skal gjøre risikovurderinger av de videoløsningene som er aktuell for deg. Du må selv vurdere om det er andre trusler som er relevante ut fra din situasjon.

Akseptkriteriene benyttet i vurderingen er hentet fra Normens faktaark 5:
https://ehelse.no/normen/faktaark/faktaark-05-fastsette-niva-for-akseptabel-risiko

K=Konfidensialitet, I=Integritet, T=Tilgjengelighet, Sa=Sannsynlighet, Ko=Konsekvens

	Trussel		**Tiltak**	**Vurdering**	
ID #	**Scenario**	**K, I, T**	**Beskrivelse**	**Sa**	**Ko**
1	Angrep inn mot virksomheten via etablerte videotjenester. Uautorisert til gang til virksomhetens data.	KIT	• Bevissthet rundt farene for misbruk av tjenestene. • Tekniske tiltak etablert i den valgt tjenesten basert på minimumskravene.	1	3
2	Manglende kapasitet i infrastruktur hos behandler. Tjenestene slutter å virke eller kvaliteten blir for dårlig.	T	• Sørge for tilstrekkelig kapasitet gjennom å skalere infrastrukturen ved behov.	1	3
3	Manglende kapasitet i infrastruktur hos videoleverandør. Tjenestene slutter å virke eller kvaliteten blir for dårlig.	T	• Velge leverandører som har prosesser for skalering av tjenestene basert på belastningen.	2	3
4	Manglende sikker autentisering av pasient eller behandler.	K	• Krav og veiledning om hvordan autentisering skal foregå. • Etablere god veiledning som kan brukes i dialog mellom pasient og behandler. • Behandler og pasient vil se hverandre.	1	2
5	Uautorisert tilgang til helseopplysninger gjennom avlytting av video	K	• Minimumskrav til tjenester om at det skal være ende- til ende kryptering.	1	3
6	Manglende kontroll på hvem som deltar i en videosesjon	K	• Krav om at det tydelig skal fremgå hvem som er med i videosamtalen. • Tydelig veiledning til behandler.	1	2

	Trussel		Tiltak	Vurdering	
ID #	**Scenario**	**K, I, T**	**Beskrivelse**	**Sa**	**Ko**
7	Falske videotjenester, eller bruk av tjenester som ikke tilfredsstiller krav.	K	• Alle med tilknytning til Helsenettet er forpliktet i henhold til Normens krav og skal gjøre egen vurdering av valgte tjenester. • Mange tjenester er i dag sperret i sentral infrastruktur hos NHN. • Internettilgang monitoreres, og falske tjenester kan avdekkes.	1	3
8	Manglende etterlevelse av krav i GDPR i løsningen. Personopplysninger behandles uten tilstrekkelig sikring eller etterlevelse av krav. Manglende innebygget personvern.	K	• Verifisere at løsningen tilfredsstiller kravene. • Gjennomføre og tilgjengeliggjøre DPIA for valgt løsning. • Forplikte leverandøren på å følge kravene i personvernforordningen.	1	2
9	Manglende logging i tjenestene	K	• For enkelte tjenester er tilstrekkelig logging etablert. • Rene kommersielle tjenester vil føre til krav om manuell logging i journal. • Det er gjeldende praksis fra f. eks. telefondialog med pasient. (Krav til journalføring).	1	2
10	Manglende sikkerhet i policy som settes på valgte løsninger. Åpner for funksjoner som ikke møter definerte minimumskrav, f. eks. opptak av video, fildeling og lignende.	K	• Benytte etablerte tjenester som oppfyller kravene. • Gode brukerveiledninger på oppsett av løsningene som publiseres lett tilgjengelig. • Anbefale å bruke lokal IT-support til oppsett av løsningene.	2	3
11	Manglende samtykke til bruk av video i pasientbehandlingen.	K	• Det er frivillig for pasienten å delta i en videokonsultasjon, og samtykket til helsehjelp gis når pasient velger å delta.	1	2
12	Lagring av video hos en av partene.	K	• Ende til endekryptering hindrer lagring av video hos leverandøren. • Klare rutiner som hindrer bruk av opptaksfunksjon der den er tilgjengelig.	1	3
13	Personopplysninger brukes til andre formål av leverandøren.	K	• Etablere tydelige krav mot leverandøren i forhold behandling av personopplysninger • Forplikte leverandøren på å følge kravene i personvernforordningen.	2	2

8 RISIKOMATRISE

Markering av hendelse i forhold til sannsynlighet og konsekvens. Rødt felt viser ikke akseptert risiko.

KONSEKVENS					
	4				
	3	1,2,5,7, 12	3,10		
	2	4,6,8,9,11	13		
	1				
		1	2	3	4
SANNSYNLIGHET					