Dato: 16.04.2020

Saksbehandler: Petter Ludvig Andersen
Ansvarlig: Birgitte Egset

Data Protection Impact Assessment (DPIA) – Personvernkonsekvensutredning etter GDPR

DEL I. Vurdering av behov for DPIA

Bruk av Skype for Business/Teams til videokonsultasjon i forbindelse med COVID -19

Det er ønskelig å raskt øke fastlegers mulighet for effektiv digital avstandsoppfølgning av innbygger/pasienter 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. Denne overordnede personvernkonsekvensvurderingen gjelder om videoløsningen Skype for Business/Teams kan benyttes som et midlertidig tiltak for å løse et prekært behov.

Når må DPIA gjennomføres?

> *«Dersom det er sannsynlig at en **type behandling**, særlig ved bruk av ny teknologi og idet det tas hensyn til behandlingens **art, omfang, formål og sammenhengen den utføres i**, vil medføre en **høy risiko** for fysiske personers **rettigheter og friheter**, skal den behandlingsansvarlige før behandlingen foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for vernet av personopplysninger.»* (GDPR art.35.1)

Kriterier når DPIA *kan* bli et krav:

1. **Evaluering eller scoring**, spesielt knyttet til arbeidsresultater, økonomisk situasjon, helse, personlige preferanser eller interesser, oppførsel og adferd, lokasjon og bevegelser osv.
2. **Automatiserte beslutninger** med juridisk eller tilsvarende betydning.
3. **Systematisk overvåking** av registrerte.
4. **Særlige kategorier personopplysninger** eller **andre sensitive personopplysninger av høy personlig karakter** (sistnevnte spesielt knyttet de enkeltes «friheter», men kan også omfatte f.eks. økonomiske og finansielle opplysninger).
5. **Databehandling i stort omfang**, som at det er et stort antall registrerte involvert, store mengder data, mange ulike typer data, lang varighet av behandlingen, stor geografisk utbredelse av behandlingen osv.
6. **Kombinering eller sammenstilling av datasett**.
7. Personopplysninger vedrørende **spesielt sårbare registrerte** (som barn, ansatte, psykisk syke, asylsøkere, eldre, pasienter mv.).
8. **Innovativ eller nyskapende bruk av personopplysninger,** som f.eks. bruk av biometriske data for tilgangskontroll, Internet of Things-løsninger, velferdsteknologi osv.
9. Når behandlingen i seg selv **forhindrer eller begrenser de registrertes mulighet til å utøve sine rettigheter** etter loven eller avtale, eller **bruke tjenester**.

Basert på Mal for DPIA utarbeidet av direktoratet for e-helse,
https://ehelse.no/personvern-og-informasjonssikkerhet/verktoy-for-implementering-av-gdpr

Vurderingsspørsmål om behov for DPIA:

Nr.	Vurderingsspørsmål	Ja/Nei
1.	Er dette et nytt prosjekt eller prosess?	Nei, videokonsultasjoner benyttes i både spesialist- og primærhelsetjenesten i dag. Denne vurderingen er utarbeidet til støtte for helsevirksomheter som vurderer å tilby videokonsultasjon ved bruk av Skype/Teams. Det kan f.eks. være aktuelt for helsepersonell som allerede har Office 365. Økt bruk av videokonsultasjon under COVID-19 krisen er et tiltak for å minimere risiko for smitte og øke kapasiteten i helsetjenesten.
2.	Vil prosjektet innebære innsamling av ny informasjon om enkeltpersoner?	Nei, direktoratet forutsetter at det eneste leverandør behandler er e-postadresse til pasient. Helsepersonellet vil behandle de samme personopplysningene som ved fysisk konsultasjon, og samle inn det som er nødvendige og relevante opplysninger for ytelsen av helsetjenesten. Dette dokumenteres i pasientens journal. I samarbeid med leverandør er det satt opp en veileder som trinn for trinn viser innstillinger i løsningen som bør settes opp før den benyttes til videokonsultasjon med pasienter. Følges denne veiledningen vil leverandøren kun behandle e-post adressen til pasienten og nødvendig logginformasjon. Ellers foregår all behandling av helse- og personopplysning hos dataansvarlige helsevirksomhet.
3.	Vil prosjektet be enkeltpersoner om å gi informasjon om seg selv?	Det er kun e-post adresse pasienten særskilt må oppgi for å gjennomføre videokonsultasjonen. Dette for å kunne motta lenke til videosesjonen. Pasienten ber om legetime/konsultasjon og helsepersonell vurderer om videokonsultasjon er egnet for å yte forsvarlig helsehjelp. Det er helsepersonell som tar initiativ til videokonsultasjonen ved å sende ut lenke.
4.	Vil informasjon om enkeltpersoner bli delt med organisasjoner eller personer som ikke tidligere har hatt rutinemessig tilgang til informasjonen?	Nei, ikke ut over e-post adressen til pasienten. Når det er aktuelt med en videokonsultasjon må e-post adressen behandles i leverandørens infrastruktur som en forutsetning for å sette opp samtalen. Selve videosamtalen er ende-ende kryptert. Veiledningen som trinn for trinn viser innstillinger i løsningen innebærer at funksjonalitet for lagring, chattfunksjonalitet etc. er skrudd av. Virksomheten må signere databehandleravtale med Microsoft for å kunne ta i bruk Skype for business/ Teams.

Nr.	Vurderingsspørsmål	Ja/Nei
		Databehandleravtalen er en del av vilkårene for bruk av Office 365.
5.	Skal du bruke informasjon om enkeltpersoner som er innsamlet for et formål, men der opplysningene for tiden ikke er eller ikke lenger er i bruk (ikke behandles utover lagring)?	Nei, formålet er å yte helsetjenester digitalt for å minimere risiko for smitte av COVID-19. Når videokonsultasjonen avsluttes lagres det ikke person- og helseopplysninger i videoløsningen. Helsepersonell må, som ved fysisk konsultasjon, journalføre relevante og nødvendige helseopplysninger fra samtalen.
6.	Innebærer prosjektet at du bruker ny teknologi som kan oppfattes som inngripende for personvernet? For eksempel, bruk av biometri eller ansiktsgjenkjenning?	Nei, teknologi som skal benyttes er Skype for business/ Teams. Videokonsultasjon benyttes i helsetjenesten i dag. Det er frivillig for pasienten å delta i en videokonsultasjon, alternativer uten fysisk oppmøte kan være telefon og skriftlig e-konsultasjon. Det er viktig å gi tilstrekkelig informasjon og det er utarbeidet informasjon om videokonsultasjon til pasienter, se lenke nedenfor.
7.	Vil prosjektet resultere i at du tar beslutninger eller gjennomfører tiltak mot enkeltpersoner på måter som kan ha en betydelig innvirkning på dem?	Nei, det er det enkelte helsepersonell som vurderer om videokonsultasjon er egnet for å gi forsvarlig helsehjelp. Dersom det ikke er det, må pasienten fortsatt inn til fysisk konsultasjon. For mange vil det å ha videodialog med fastlege og annet helsepersonell i nåværende situasjon, være en sikkerhet i seg selv mtp. risiko for smitte.
8.	Basert på typen informasjon om enkeltpersoner, er det spesielt sannsynlig at bekymringen for eller forventninger til personvernet vil øke?	Nei, behandling av helseopplysninger foregår på samme måte som ved en fysisk konsultasjon, eller en telefonkonsultasjon, hvor helsepersonell dokumenterer helsehjelpen i pasientens journal. E-post adressen til pasienten vil lagres i utboksen hos helsepersonell. Dette er informasjon som viser at det har vært en kontakt mellom pasient og helsepersonell, f.eks. dersom e-post adressen inneholder fullt navn. Informasjonen lagres i henhold til vilkårene for bruk av Office 365.
9.	Vil prosjektet kreve at du kontakter personer på måter som de kan finne inngripende?	Nei, pasient og helsepersonell vil på forhånd avtale videokonsultasjon. Pasient får lenke til konsultasjonen på e-post fra helsepersonell. Det er frivillig for pasienten å delta.

Konklusjon:

Videoløsningen Skype for Business/Teams er vurdert ut fra noen minimumskrav til sikkerhet, se nedenfor. Leverandøren har utarbeidet en veileder som trinn for trinn viser innstillinger i løsningen som bør settes opp før den benyttes til videokonsultasjon med pasienter fordi det minimer personvernkonsekvenser. Det er viktig å bemerke at løsningen er å anse som et midlertidig tiltak for å løse et prekært behov for økt kapasitet for videokonsultasjon i helsetjeneste. Det kan være risikoer som ikke er adressert som følge av dette.

Forutsatt at de mest personvernvennlige innstillingene settes opp før bruk, vil leverandør bare behandle e-post adresse til pasient for å kunne sette opp og gjennomføre konsultasjonen. Denne behandlingen innebærer ikke en høy risiko for fysiske personers rettigheter og friheter og det er derfor ikke krav om å gjennomføre en fullverdig vurdering av personvernkonsekvenser etter GDPR artikkel 35. Helsepersonell som skal tilby videokonsultasjon vil fortsatt behandle helse- og personopplysninger på samme måte som ved en fysisk konsultasjon og dokumenterer behandlingen av helse- og personopplysninger i pasientens journal.

Direktoratet for e-helse vil påpeke at det uansett er viktig å gi tilstrekkelig informasjon til pasient slik at de kan håndheve sine rettigheter etter helselovgivningen og personvernregelverket.

Tilknyttet informasjon:

- https://ehelse.no/aktuelt/korona-slik-kommer-du-i-gang-med-videokonsultasjon med lenke til mer informasjon, herunder roverordnet ROS
- Trinn for trinn veiledning for å komme i gang, utarbeidet av Microsoft
- Informasjon til pasienten ved videokonsultasjon

Følgende minimumskrav er lagt til grunn:

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. Norske medier har allerede meldt om ondsinnede aktører som utnytter sårbarheten vi står ovenfor gjennom phisingangrep.

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.

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 kryptering betyr det at dersom en uautorisert aktør stjeler lenke, vil ikke vedkommende kunne nyttegjøre seg av lenken.

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.

Personvernforordningen

Leverandør av videotjenesten skal kunne forplikte seg til å etterleve kravene i personvernforordningen (GDPR).