NORMEN

Informasjonssikkerhet og personvern ved bruk av teknologi i kommuner (velferdsteknologi)

Versjon 3.0

Utgitt med støtte av:

Direktoratet for e-helse

Endringshistorikk for og godkjenning av dokumentet

Versjon	Endringer	Godkjent av styringsgruppen for Normen (dato)
1.0	Første utgave av veilederen	02.03.15
2.0	Andre utgave av veilederen med følgende endringer: - Behandler kun informasjonssikkerhet som er spesielt for velferdsteknologi. - Personvern er tatt ut - Veilederen dekker ikke veiledning i juridiske problemstillinger (dokumentasjon, samtykke, avstandsoppfølging mv.). Se kapittel 1.3 Avgrensning - Veilederen struktureres som en tenkt prosess fra ide til anskaffelse i kap. 2 - Det er gitt fire nye eksempler - Tekst er skrevet om for å rendyrke det som er spesielt for velferdsteknologi pg gi referanser til mer informasjon i faktaark og veiledere - Personvernforordningen (GDPR) omtales. Se kap. 3 - Endret layout: Kursiv og definisjoner er borte ny font, økt bruk av bilder og illustrasjoner	08.06.17
3.0	Tredje utgave av veilederen med følgende endringer: - Tatt inn personvern - Omhandler mer veiledning om juridiske problemstillinger - Skrevet om kommunens, leverandørers, databehandlere, og andres ansvar - Veiledning om personvernkonsekvensvurderinger	17.09.20

INNHOLD

1. Innledning

1.1. Hvorfor er informasjonssikkerhet og personvern avgjørende for forsvarlig helse- og omsorgstjenester

For å kunne yte forsvarlige helse- og omsorgstjenester er det avgjørende at riktige og oppdaterte opplysninger om pasientene og brukerne er tilgjengelige på rett sted til rett tid. Helsepersonell må ha tillit til at opplysningen er korrekte og fullstendige, og helse- og omsorgstjenesten er avhengig av tillit fra befolkningen for at pasienter, brukere og pårørende vil dele sensitive og personlige opplysninger med tjenestene.

Kommunen skal sørge for at opplysningene ivaretas, brukes og behandles på en sikker måte. Relevant og nødvendig informasjon skal være tilgjengelig for de som har tjenstlig behov og uvedkommende skal ikke ha tilgang. informasjonen skal være korrekt og oppdatert.

Det er opp til kommunen å vurdere om et tjenestetilbud skal inneholde velferdsteknologi. Den som mottar tjenestene har rett til å medvirke i utformingen av tjenestetilbudet.

Ved innføring av velferdsteknologi i tjenestene møter kommuner på mange spørsmål som gjelder behandling av helse- og personopplysninger. Selv om behandling av helse- og personopplysninger ikke er nytt innenfor helse- og omsorgstjenesten, kan noen problemstillinger oppleves større og annerledes enn før.

- Bruk av velferdsteknologi generer mye informasjon om pasienter og brukere, og det må vurderes om innsamling og lagring av informasjonen er relevant og nødvendig for tjenesteytingen. Dette stiller krav til kunnskap om dokumentasjonsplikt, herunder taushetsplikten og unntak fra denne.
- Det er mange aktører involvert i behandling av helse- og personopplysninger, og opplysninger blir delt med ulike aktører som alarmsentraler/ responssentre, tekniske enheter og kommunikasjons- og utstyrsleverandører m.fl. Dette krever kunnskap om roller og ansvar ved behandling av opplysninger, herunder krav til taushetsplikt, behov for databehandleravtaler osv.
- EUs personvernforordning (GDPR) krever bl.a. at det gjøres personvernkonsekvensvurderinger (DPIA) når man innfører teknologi som involverer behandling av helse- og personopplysninger.
- Detaljerte opplysninger om pasient/ brukere, pårørende og ansatte gir risiko for bruk av opplysninger andre/ nye og uforenlige formål. Dette krever kunnskap og bevissthet om dataansvar, personvernprinsipper og hva som er lovlig bruk av opplysningene.
- I økende grad plasseres eller installeres velferdsteknologiske hjelpemidler i pasientens/ brukerens hjem. Dette åpner for nye risikoer som må kartlegges og håndteres.

For at kommunen skal kunne yte forsvarlige helse- og omsorgstjenester må informasjonssikkerhet og personvern være ivaretatt i teknologien som brukes. Dette er temaet for denne veilederen.

1.2. Om veilederen og avgrensinger

Tema for denne veilederen er personvern og informasjonssikkerhet ved bruk av velferdsteknologiske løsninger. Veilederen tar også for seg risiko og risikoscenarier for ulike typer velferdsteknologi, samt ulike temaer innen personvern og informasjonssikkerhet, juridiske spørsmål, sentrale prosesser og tiltak. Videre gis det veiledning om reglene i personvernforordningen (GDPR) som vil kunne innebære at det stilles krav om at det skal gjennomføres risikovurderinger, personvernkonsekvensvurderinger (DPIA), at behandlinger av helse- og personopplysninger skal føres i en oversikt (protokoll) og at løsningene for velferdsteknologi skal ha innebygd personvern. Veilederen er en støtte i arbeidet med utvikling, innføring og drift av teknologi i kommunale helse- og omsorgstjenester.

Veilederen er ikke uttømmende om temaer innen velferdsteknologi. Veilederen omfatter i noen grad helselovgivningens alminnelige regler for behandling av helse- og personopplysninger. Temaer som taushetsplikt, dokumentasjonsplikt, kommunikasjon av opplysninger og pasient- og brukerrettigheter dekkes ikke av denne veilederen. For veiledning om disse temaer vises det til følgende veiledninger og rundskriv:

- Helsepersonelloven med kommentarer
- Pasient- og brukerrettighetsloven med kommentarer
- Helsepersonells og forvaltningens taushetsplikt
- Veileder for saksbehandling av tjenester etter helse- og omsorgstjenesteloven

Veilederen omtaler ikke bruk av videokommunikasjon. For temaer innen video kan disse veilederne benyttes:

- Veileder i video-, lyd og bildeopptak: https://ehelse.no/normen/veiledere/veileder-video-lyd-og-bildeopptak-i-helse-og-omsorgssektoren
- Faktaark 54 – videokonsultasjon: https://ehelse.no/normen/faktaark/faktaark-54-videokonsultasjon
- Kvikk-guide for videokommunikasjon: https://www.ks.no/fagomrader/helse-og-omsorg/velferdsteknologi3/kvikk-guide-for-videokommunikasjon/

Normen har en veileder for bruk av portalløsninger, SMS og e-post som kan være til hjelp om kommunen benytter portalløsninger, SMS eller e-post i kommunikasjon med pasient/bruker når de tar i bruk velferdsteknologi: https://www.ks.no/fagomrader/helse-og-omsorg/velferdsteknologi3/kvikk-guide-for-videokommunikasjon/

For mer veiledning om bruk av skytjenester i kombinasjon med velferdsteknologi kan veileder i bruk av skytjenester være til hjelp: https://ehelse.no/normen/veiledere/veileder-i-bruk-av-skytjenester-til-behandling-av-helse-og-personopplysninger

I veilederen benyttes det enkelte uttrykk og definisjoner som er spesifikke for fagdisiplinene informasjonssikkerhet og personvern. Se Normens definisjonskapittel (kap. 6.1) og om Normen for definisjon på informasjonssikkerhet (kap. 1) for forklaring.

1.3. Veilederens forhold til andre dokumenter og veiledere

Det finnes flere veiledere og dokumenter som omhandler bruk av velfersteknologi og nærmere om vurderinger av personvern og informasjonssikkerhet. Sammen med denne veilederen er det et godt utgangspunkt å lese følgende veiledere utarbeidet av Nasjonalt velferdsteknologiprogram. Til sammen danner disse et godt utgangspunkt for basiskunnskap om personvern og informasjonssikkerhet:

- Kvikk-guide til velferdsteknologi: https://www.ks.no/globalassets/kvikk-guide-ny.pdf
- Kvikk-guide til behandling av helse- og personopplysninger ved bruk av velferdsteknologi: https://www.ks.no/fagomrader/helse-og-omsorg/velferdsteknologi3/behandling-av-helse--og-personopplysninger-ved-bruk-av-velferdsteknologi/
- Kvikk-guide til anskaffelse av velferdsteknologi https://www.ks.no/fagomrader/innovasjon/innovasjonsledelse/veikart-for-tjenesteinnovasjon/kvikk-guide-til-anskaffelser-av-velferdsteknologi/

Helse- og omsorgstjenesten i kommunen må ivareta en rekke oppgaver i tett samarbeid med teknisk avdeling, IT, innkjøp og andre. Nasjonalt velferdsteknologigprogram har utarbeidet en helhetlig tjenestemodell for velferdsteknologi som inneholder en rekke oppgaver som må løses. I dokumentet gis det veiledning om organisering av tjenesten, oversikt over oppgavene som må utføres, og eksempler på hvordan andre kommuner løser dem: https://www.ks.no/contentassets/95055368c1ef41b1a1050e5df08b590a/Helhetlig-tjenestemodell-for-velferdsteknologi-.pdf

En annen nyttig veileder for kommuner som arbeider med velfersteknologi er Normens veileder for bruk av medisinsk utstyr/ behandlingshjelpemidler: https://ehelse.no/normen/veiledere/veileder-i-personvern-og-informasjonssikkerhet-medisinsk-utstyr

1.4. Om Normen

Denne veilederen er et støttedokument under Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen) som forvaltes av Styringsgruppen for Normen. Gjeldende utgave av Normen bygger på regelverket i personopplysningsloven, personvernforordningen og helselovgivningen.[1]

Normen skal bidra til tilfredsstillende informasjonssikkerhet og personvern i den enkelte virksomhet og i sektoren generelt. I tillegg skal Normen bidra til å etablere mekanismer og regler som sikrer at kommuner og samarbeidende virksomheter i helse- og omsorgssektoren kan ha gjensidig tillit til at behandling av helse- og personopplysninger gjennomføres på et forsvarlig sikkerhetsnivå.

For en komplett oversikt over Normens krav og andre nyttige dokumenter, se mer via denne lenken: https://ehelse.no/normen/oversikt-over-normens-krav-og-mapping-mellom-iso-og-normen

Dersom du har spørsmål knytte til veilederen kan du sende spørsmål og kommentarer til: sikkerhetsnormen@ehelse.no

[1] https://ehelse.no/normen/normen-for-informasjonssikkerhet-og-personvern-i-helse-og-omsorgssektoren

2. Noen juridiske problemstillinger

Ytelse og administrasjon av helse- og omsorgstjenester forutsetter at kommunen behandler helse- og personopplysninger om pasient/ bruker. Dokumentasjon av nødvendige og relevante opplysninger skal bidra til at pasienter og brukere får helse- og omsorgstjenester av god kvalitet, og være til støtte for helsepersonell ved ytelse av helse- og omsorgstjenester. Ivaretakelse av pasientens/ brukerens personvern er viktig bl.a. ved at journalopplysningene er relevante, korrekte og oppdatert . I tillegg til at teknologien som benyttes har et tilstrekkelig sikkerhetsnivå er viktig for pasient- og brukersikkerheten.

Det kan være utfordrende å se forholdet mellom personvernregelverket og helselovgivningen. Via Personopplysningsloven er personvernforordningen inkorporert i norsk rett, og gir samlet de overordnede reglene om behandling av personopplysninger i alle sektorer. Helselovgivningen, særlig helsepersonelloven, pasientjournalloven og helseregisterloven, utfyller og supplerer reglene i personvernforordningen ved behandling av personopplysninger i helse- og omsorgssektoren.

2.1. Behandlingsgrunnlag

Personopplysninger kan bare behandles når lovgivningen tillater det som betyr at all behandling av personopplysninger skal ha et lovlig grunnlag. I personvernforordningen kalles dette et behandlingsgrunnlag. Det lovlige grunnlaget kan finnes i andre lover enn personvernforordningen. Behandlingsgrunnlaget skal dekke alle typer behandlinger av helse- og personopplysninger som utføres: innsamling, registrering, lagring, sletting, utlevering, mv.

Det er flere alternative behandlingsgrunnlag i forordningen. Noen av dem stiller krav om at behandlingen er lovlig som følge av annen lovgivning. Dette kalles supplerende rettsgrunnlag. Dokumentasjonsplikten i helsepersonelloven, og forsvarlighetskravet som nødvendiggjør dokumentasjonen, utgjør et slikt supplerende rettsgrunnlag for behandling av helseopplysninger om pasient. I tillegg til dokumentasjonsplikten og forsvarlighetskravet, inneholder helselovgivningen også regler om annen behandling av opplysninger, herunder taushetsplikt og bruk av opplysninger til intern og ekstern kvalitetssikring, forskning mv.

Utgangspunktet for å kunne dokumentere helse- og personopplysninger i helse- og omsorgstjenesten, er at opplysningene er nødvendige for å kunne yte eller administrere helse- og omsorgstjenester. Dokumentasjon av opplysninger for andre formål, eller innenfor andre sektorer (f.eks. på skolen eller i barnevernet) må ha et annet behandlingsgrunnlag, enten i sektorlovgivningen eller direkte i personvernforordningen.

2.1.1 Spesielt om bruk av samtykke

Samtykke er et viktig begrep både ved ytelse av helse- og omsorgstjenester og ved behandling av personopplysninger, og kan utgjøre rettsgrunnlag i begge tilfeller. Samtykke er også et mye brukt begrep ute i tjenesten i forbindelse med bruk av velferdsteknologi. Dette har vist seg å være en utfordring for mange, og det har vist seg å være lett å blande disse samtykkene da det stilles ulike krav ut fra hvilke samtykke det dreier seg om, noe som kan skape mye usikkerhet.

Rettsgrunnlag for ytelse av helse- og omsorgstjenester (med eller uten velferdsteknologi) og rettsgrunnlag for å behandle personopplysninger er ulikt regulert. Nedenfor går vi igjennom de viktigste reglene.

2.1.1.1 Ytelse av helse- og omsorgstjenester[2]

Helse- og omsorgstjenester kan i utgangspunktet bare ytes når tjenestemottakeren samtykker til dette. For helsehjelp følger det av pasient- og brukerrettighetsloven § 4-1, men det gjelder også innenfor omsorgstjenestene basert på ulovfestet rett og alminnelige rettsprinsipper.

Utgangspunktet er at dette samtykket gis implisitt, dvs. uten at det sies uttrykkelig. Typisk skjer dette ved at pasienten eller brukeren møter opp hos legen eller slipper tjenesteyterne inn i sitt hjem, og før øvrig samarbeider med legen/tjenesteyteren, og dermed gjennom sin atferd viser at han eller hun samtykker til helsehjelpen/tjenestene. Dette gjelder uavhengig av om tjenestene ytes med eller uten bruk av velferdsteknologi. Det er med andre ord ikke nødvendig med samtykkeerklæringer som må leses og underskrives.

Selv om samtykket ikke behøver å være uttrykkelig, må det likevel være informert. Med det menes at personen må ha fått tilstrekkelig informasjon om tilbudet/ tjenesten til å vite hva hun eller han "er med på", enten tjenesten ytes med eller uten bruk av velferdsteknologi. Jo mindre det kan forventes at pasienten eller brukeren vet om den aktuelle helsehjelpen/ tjenesten/ teknologien fra før, jo bedre må det informeres.

Hvis pasienten/brukeren vurderes å ikke være samtykkekompetent, må det implisitte samtykket erstattes med et annet rettslig grunnlag. Følgende lovhjemler kan da være aktuelle:

- pasient- og brukerrettighetsloven § 4-6
- pasient- og brukerrettighetsloven § 4-6a
- pasient- og brukerrettighetsloven kapittel 4A
- helse- og omsorgstjenesteloven kapittel 9.

2.1.1.2 Behandlingsgrunnlag for behandling av helse- og personopplysninger

Behandlingsgrunnlaget for behandling av nødvendige og relevante helse- og personopplysninger i helse- og omsorgstjenesten er dokumentasjonsplikten og plikten til å sikre at de tjenestene som tilbys og ytes er forsvarlige. Det gjelder også når tjenestene ytes ved hjelp av velferdsteknologi.

---

[2] Les mer om samtykke til helse- og omsorgstjenester her: https://www.helsedirektoratet.no/rundskriv/pasient-og-brukerrettighetsloven-med-kommentarer/samtykke-til-helsehjelp

Hvis en virksomhet benytter samtykke til behandling av helse- og personopplysninger når de yter helse- og omsorgstjenester kan dette skape utfordringer for virksomheten dersom tjenestemottakeren trekker tilbake sitt samtykke. Etter kravene i personvernforordningen skal opplysningene som virksomheten har samlet inn da slettes, men dersom virksomheten gjør dette fører det til brudd på helselovgivningens krav til dokumentering av ytelsene av helse- og omsorgstjenester. Derfor kan ikke samtykke til behandling av helse- og personopplysninger benyttes i slike tilfeller.

Samtykke ved behandling av helse- og personopplysninger kan f.eks. være aktuelt i enkelte av kommunens tjenester der dette ikke er tjenester som er hjemlet i lovgivning, som noen forebyggende tjenester. Samtykke er også et aktuelt behandlingsgrunnlag ved forskning og gjenbruk av data. Eksempler på slike kommunale tjenester kan være treningstilbud for eldre, samtalegrupper o.l.

Hvis behandlingsgrunnlaget skal være samtykke, må samtykke innhentes. Et samtykke til behandling av helse- og personopplysninger må være eksplisitt/ uttrykkelig; dvs. at i motsetning til det som gjelder for samtykke til helse- og omsorgstjenester kan ikke passivitet, stillhet o.l. utgjøre et gyldig samtykke. Les mer om veiledning for bruk av samtykke hos Datatilsynet: https://www.datatilsynet.no/rettigheter-og-plikter/kommunenes-plikter/behandlingsgrunnlag/veileder-om-behandlingsgrunnlag/samtykke/

Les mer om de ulike behandlingsgrunnlagene i Normen: https://ehelse.no/normen/normen-for-informasjonssikkerhet-og-personvern-i-helse-og-omsorgssektoren#4.1%20Behandlingsgriunnlag

Eksempel – Samtykke

Normland kommune skal implementere ny elektronisk medisineringsstøtte. De lurer på om de trenger samtykke fra tjenestemottakerne?

Det første Normland kommune må spørre seg om er: samtykke til hva?

1. Å gi medisiner er en del av helsehjelpen som Normland allerede yter til disse tjenestemottakerne. Rettsgrunnlaget for denne helsehjelpen er (implisitt) samtykke. Samtykke til helsehjelp er på plass.
2. Siden dette er helsehjelp som Normland skal yte må de også dokumentere denne helsehjelpen og sikre at helsehjelpen er forsvarlig. Dette kan Normland gjøre med hjemmel i lov, dvs. at loven gir dem anledning til å behandle tjenestemottakernes personopplysninger. De trenger derfor i**kke** samtykke for å behandle personopplysningene.

Normland må huske på at selv om tjenestemottakeren ikke trenger å signere på et samtykkeskjema må hun fremdeles få god informasjon om hvordan personopplysningene hennes behandles.

3. Leverandøren som har levert utstyret vil gjerne bruke personopplysningene i et prosjekt de har sammen med Normsund høyskole. Normland kommune må vurdere om dette har samme formål som helsehjelpen. Det kommer de frem til at det ikke er. De kan ikke bruke dokumentasjonsplikten og helselovgivningens regler om ytelse av helse- og omsorgstjenester for å gi leverandøren og Normsund fylkeskommune lov til å behandle personopplysningene. Da må de vurdere nytt behandlingsgrunnlag for dette. Det kan være samtykke. Men det er IKKE en del av den ordinære tjenesten elektronisk medisineringsstøtte.

Normland kommunes nabokommune, Normvik, deler i et samarbeidsprosjekt at de tidligere innhentet samtykke for behandling av personopplysninger ved all velferdsteknologi. De fikk en vanskelig sak for en stund siden da brukeren trakk sitt samtykke og ville at alle opplysningene om henne skulle slettes. Men sletting var umulig da dette var personopplysninger som måtte journalføres. Normvik var veldig glade for at de hadde lest i en veileder at det som hovedregel ikke var behov for samtykke til behandling av personopplysninger i velferdsteknologi.

2.1.1.3 Inngripende teknologi

Inngripende teknologi er all sporings-, varslings-, lokaliserings- og overvåkningsteknologi som sender informasjon til en tredjepart om pasientens eller brukerens handlinger, bevegelser, oppholdssted e.l. uten at pasienten eller brukeren selv initierer det.

Hvis teknologien er inngripende, må det vurderes hvilket rettsgrunnlag for ytelse av helse- og omsorgstjenester som er det aktuelle, og om det må fattes vedtak (se Velferdsteknologiens ABC hefte C, Lovverk og etikk).
https://www.helsedirektoratet.no/veiledere/saksbehandling-av-tjenester-etter-helse-og-omsorgstjenesteloven

2.2. Særlig om journalføring/dokumentasjon av relevante og nødvendige opplysninger fra velferdsteknologiske løsninger

Det er den som yter helsehjelp som skal nedtegne/ registrere relevante og nødvendige opplysninger om pasienten og helsehjelpen i en pasientjournal for den enkelte pasient etter reglene i helsepersonelloven §§ 39 og 40.

Ved utvikling og bruk av velferdsteknologi kan det oppstå behov for standardiserte vurderinger av hva som er relevant og nødvendig. Men også ved bruk av velferdsteknologi i helse- og omsorgstjenesten skal det gjøres en individuell vurdering av hva som er nødvendige og relevante opplysninger for den enkelte bruker/ pasient. Hvis velferdsteknologiske løsninger skal sende informasjon automatisk inn i journalen må løsningene kunne konfigureres slik at det kun er relevant og nødvendig informasjon som blir sendt over.

Ved bruk av digitalt tilsyn/ GPS/ trygghetsalarm kan en overordnet rapportering om hvordan tiltaket (bruken av teknologien) fungerer, og dokumentasjon av den personelloppfølgingen som skjer i utgangspunktet være tilstrekkelig. I enkelte tilfeller kan det være behov for mer. Dette må baseres på en konkret vurdering for den enkelte pasient.

For digital hjemmeoppfølging vil det være store variasjoner i hva som er relevant og nødvendig informasjon og dermed hva som skal journalføres i de ulike situasjonene. Dette må helsepersonell vurdere i hvert enkelt tilfelle.

Ved bruk av elektronisk medisineringsstøtte/ medisindispenser vil det være behov for at ansvarlig helsepersonell avgjør hva som skal journalføres. I mange tilfeller kan det f.eks. være nødvendig å journalføre at medisinene i dispenseren er tatt til rett tid. Det samme vil være gjeldende for eventuelle meldinger om avvik som krever oppfølging av helsepersonell. Dette skal vurderes konkret.

2.3. Gjenbruk av data til kvalitetssikring og forskning

Det samles inn mer og mer data fra ulike typer teknologi som benyttes i helse- og omsorgstjenestene. Med det følger også et større ønske og et behov for å benytte data til både kvalitetssikring og forskning.

2.3.1 Kvalitetssikring

Når formålet er læring og kvalitetssikring for helsepersonell som tidligere har ytet helsehjelp eller omsorgstjenester til pasienten i et konkret behandlingsforløp kan det tilgjengeliggjøres taushetsbelagte helseopplysninger, selv om vedkommende 4ikke skal medvirke i den videre ytelsen av helsehjelp eller andre omsorgstjenester. Dette kan bare skje hvis pasienten ikke motsetter seg det.

Dette omfatter situasjoner der kommunen skal kvalitetssikre tjenesten. Som f.eks. bruken av elektronisk medisineringsstøtte, om det gis riktig medisinering til riktig tid, eller om hvorvidt GPS-lokalisering av pasienter med demens er riktig bruk av den spesifikke teknologien. Ved å få opplysningene kan behandler vurdere om undersøkelsene, vurderingene og behandlingstiltakene som ble gjort var korrekte, eller om andre tiltak må iverksettes. Dette gjelder også valg av teknologi i den spesifikke tjenesten teknologien benyttes.

Det kan være aktuelt å bruke de dokumenterte opplysningene til noe annet enn ytelse og administrasjon av helse- og omsorgstjenester, f.eks. kvalitetssikring eller forskning. I noen tilfeller kan det også være ønskelig å ta vare på overskuddsinformasjon fra teknologien. Da må dette ha et annet behandlingsgrunnlag. Et slikt behandlingsgrunnlag kan være samtykke, eller annen hjemmel i personvernforordningen, evt. supplert av hjemmel i lov.

Helsedirektoratet har utarbeidet et rundskriv hvor de gjennomgår helsepersonellovens § 29c om opplysninger til bruk i læringsarbeid og kvalitetssikring som det anbefales at kommunen leser: https://www.helsedirektoratet.no/rundskriv/helsepersonelloven-med-kommentarer/taushetsplikt-og-opplysningsrett/-29c.opplysninger-til-bruk-i-laeringsarbeid-og-kvalitetssikring

2.3.2 Forskning

Data innsamlet fra velferdsteknologi kan være verdifull for forskning både for kommunen, leverandør og andre. Det er viktig at kommunen kan identifisere problemstillinger som gjelder forskning og henter inn kompetanse dersom dette trengs.

Når kommunen ønsker å forske på helseopplysninger som er samlet inn via velferdsteknologi må man ha et selvstendig behandlingsgrunnlag. Kommunen kan ikke bruke dokumentasjonsplikten som behandlingsgrunnlag. Forskning er et annet formål og krever derfor et eget behandlingsgrunnlag. Dette kan f.eks. være samtykke, lovhjemmel eller annet. Virksomheten må gjøre en konkret vurdering.

For medisinsk og helsefaglig forskning må kommunen etterleve kravene i helseforskningsloven. For innsamling av opplysninger til å fremme helse, forebygge sykdom, og gi bedre helse- og omsorgstjenester følger bestemmelsene i helseregisterloven. For begge disse forskningsområdene skal behandlingen av helseopplysninger være i samsvar med prinsippene i personvernforordningen artikkel 5 (se Normens kapittel 2.2). Gjennomføring av en personvernkonsekvensvurdering (DPIA) kan bidra til at kommunen følger personvernprinsippene. Se mer i kapittel 6.3.

I tillegg er det presisert i lovene at graden av personidentifikasjon for helseopplysningene ikke skal være større enn nødvendig for å oppnå formålene med forskning. Dette betyr at om mulig bør man forske på opplysninger som er anonymiserte eller pseudonymiserte (gjort indirekte identifiserbare).

Noen forskningsprosjekter må godkjennes hos Regional etisk forskningskomite (REK)[3]. Forskningsleder/ ansvarshavende skal søke om forhåndsgodkjenning av:

- Medisinske og helsefaglige forskningsprosjekter
- Generelle forskningsbiobanker
- Dispensasjon fra taushetsplikt med hjemmel i forvaltningsloven §13d og helsepersonelloven §29 1.ledd, for annen type forskning

[3] Les mer om dette på rekportalen.no og etikkom.no

3. Medisinsk utstyr

I større grad implementerer kommunene velferdsteknologiske løsninger som er klassifisert som medisinsk utstyr. Med medisinsk utstyr regner alle instrumenter, apparater, utstyr, programvare, implantat, reagens, materiale eller andre gjenstander som ifølge produsenten er beregnet på å bli brukt, alene eller i kombinasjon, på mennesker med ett eller flere spesifikke medisinske formål. Dette inkluderer utstyr som brukes til diagnostisering, forebygging, overvåking, prediksjon, prognostisering, behandling eller lindring av sykdom, skade eller ved funksjonshemming. I tillegg vil tilbehør av medisinsk utstyr som blir brukt sammen med eller med flere medisinske utstyr som f.eks. programvaren i utstyret, eller en skytjeneste som mottar data fra utstyret, klassifiseres som medisinsk utstyr.

Det finnes flere tilfeller hvor velferdsteknologi er klassifisert som medisinsk utstyr. For eksempel kan elektronisk medisineringsstøtte, blodsukkerapparater, blodtrykksmålere, pulsmålere og aktivetsmåler klassifiseres som medisinsk utstyr.

Når det behandles helse- og personopplysninger i det medisinske utstyret vil personvernforordningen gjelde på samme måte som ved all annen behandling av helse- og personopplysninger. Dette betyr at ved behandling av helse- og personopplysninger i utstyret er det kommunen som er ansvarlig.

Les mer i Normens veileder for informasjonssikkerhet og personvern i medisinsk utstyr: https://ehelse.no/normen/veiledere/veileder-i-personvern-og-informasjonssikkerhet-medisinsk-utstyr

3.1. Krav til elektroniske programbare systemer

Det følger en rekke krav til elektroniske programbare systemer i forordningen om medisinsk utstyr (utstyr som inneholder programbare systemer og programvare som er utstyr i seg selv) som **produsenten** skal etterleve.

- Utstyret skal designes slik at det sikres at repeterbarhet, pålitelighet og ytelse er i samsvar med den tiltenkte bruken. Ved feil i utstyret, skal det treffes egnede tekniske tiltak slik at risikoene eller den svekkede ytelsen som dette kan innebære, fjernes eller reduseres så langt som mulig.
- Utstyret skal utvikles og framstilles i samsvar med det aktuelle tekniske nivået, idet det tas hensyn til prinsippene for utviklingslivssyklus, risikohåndtering (herunder informasjonssikkerhet, verifisering og validering).
- Utstyr som er beregnet på bruk i kombinasjon med mobile databehandlingsplattformer skal utvikles og framstilles ved at det tas høyde for den mobile plattformens særlige egenskaper (f.eks. skjermens størrelse og kontrastforhold), og ytre faktorer knyttet til bruk (skiftende lys- eller støynivå i omgivelsene).
- Produsenter av utstyret skal fastsette minstekrav til maskinvare, IT-nettverkenes egenskaper og IT-sikkerhetstiltak (vern mot uautorisert tilgang, som er nødvendige for å kunne bruke programvaren som beregnet).[4]

[4] EU2017/745 av 5 april 2017 om medisinsk utstyr vedlegg 1, kapittel 2 nr. 17.

Medical Device Coordination Group (MDCG) har utarbeidet en veileder for cybersikkerhet i medisinsk utstyr på bakgrunn av EU-forordning for medisinsk utstyr: https://ec.europa.eu/docsroom/documents/38941

3.2. Velferdsteknologi som medisinsk utstyr

Kommunen må undersøke om utstyret er klassifisert som medisinsk utstyr. Dette kan leverandøren svare på. Kommunen er selv ansvarlig for å anskaffe medisinsk utstyr som samsvarer med kravene som stilles til produsentene og som er egnet for det tiltenkte bruksområdet.[5]

Forordningen for medisinsk utstyr (MDR) har på lik linje som personvernforordningen en risikobasert tilnærming. I MDR brukes begrepet pasientsikkerhet, men også her må produsenten inkludere informasjonssikkerhet i risikovurderingene, selv når informasjonssikkerheten ikke er direkte nevnt i bestemmelsene. Flere og flere typer medisinsk utstyr kobles til nettverk og gjøres digitalt. Basert på dette øker også risikoen for brudd på informasjonssikkerheten og personvern.

Operatører og brukere som inkluderer helsepersonell og pasient/ bruker er ansvarlige for å bruke det medisinske utstyret basert på instruksjonene fra produsenter.

[5] Forskrift om håndtering av medisinsk utstyr

4. Ansvar, styring og ledelse

4.1. Kommunens ansvar

Kommunens øverste ledelse har ansvaret for å sørge for at kommunen følger gjeldende krav til informasjonssikkerhet og personvern ved ytelse av helse- og omsorgstjenester.

Ledelsen kan delegere myndigheter og oppgaver nedover i organisasjonen. Dette må dokumenteres i kommunens styringssystem/ internkontrollsystem og være synlig og tilgjengelig for alle. F.eks. må ansvaret for å gjennomføre og følge opp risikovurderinger tydelig plasseres for å sikre at risikovurderinger gjennomføres og at de ikke gjøres flere steder.

Kommunen er dataansvarlig for velferdsteknologiske løsninger. Dataansvarlig er den som alene eller sammen med andre virksomheter bestemmer formålet med behandlingen av helse- og personopplysninger og hvilke midler som skal benyttes. I personvernforordningen benyttes begrepet behandlingsansvarlig, som er det samme som dataansvarlig i helsesektoren.

Kommunens ledelse skal sørge for at

- det føres oversikt over behandlinger av helse- og personopplysninger[6]
- det finnes rutiner for å oppfylle de registrertes rettigheter
- medarbeidere gis opplæring og har tilstrekkelig kompetanse[7]
- kommunen har et styringssystem for informasjonssikkerhet(ISMS)[8]
- avvik behandles og håndteres[9]
- kommunen ivaretar sitt behandlingsansvar for ytelse av helsehjelp
- gjennomføre ROS-vurderinger[10] og personvernkonsekvensvurdering[11]
- etablere og dokumentere tekniske og organisatoriske tiltak
- inngå og følge opp avtaler

Kommunen skal sørge for at de har tilgjengelig tilstrekkelige ressurser og kompetanse til å innføre og følge opp velferdsteknologi. Dette betyr at det må være tilgjengelig kompetanse innen både juridisk, sikkerhet, personvern, helse, IT, drift mv.

Innføring av velferdsteknologi kan være organisert som prosjekt. Det daglige ansvaret følges da opp av en prosjektleder. Det må sikres tett kontakt mellom prosjektet og kommunens øvrige roller innen informasjonssikkerhet, personvern og helsefag.

---

66 https://ehelse.no/normen/faktaark/faktaark-13-protokoll-over-behandlinger-av-helse-og-personopplysninger-i-virksomheten
7 https://ehelse.no/normen/faktaark/faktaark-09-opplaering-av-ledere-og-medarbeidere
8 https://ehelse.no/normen/faktaark/faktaark-02-styringssystem-for-informasjonssikkerhet-og-personvern
9 https://ehelse.no/normen/faktaark/faktaark-08-avviksbehandling
10 FA 07 Risikovurdering
11 Mal for DPIA: https://ehelse.no/personvern-og-informasjonssikkerhet/verktoy-for-implementering-av-gdpr

4.2. Leverandør/ databehandlers ansvar

Leverandør av velferdsteknologi til kommunen har ikke et selvstendig ansvar for at teknologien ivaretar kravene i lovverket. Kommunen må derfor stille krav til leverandøren om etterlevelse av regelverk i kravspesifikasjoner, avtaler mv. og sørge for at løsningen blir dokumentert.[12]

Se mer om anskaffelse av utstyr i kapittel 4.3

4.2.1 Bruk av databehandler og databehandleravtale

En databehandler er en virksomhet som behandler helse- og personopplysninger på vegne av dataansvarlig. Når kommunen benytter en leverandør til et oppdrag, vil ikke denne leverandøren nødvendigvis være databehandler. Det er kun når leverandør skal behandle helse- og personopplysninger på vegne av kommunen at det foreligger et databehandlerforhold. Hvis leverandøren f.eks. bare får tilgang til opplysninger, men ikke skal behandle dem, vil det være tilstrekkelig med taushetserklæring.

Når andre behandler helse- og personopplysninger på vegne av kommunen, skal dette reguleres i en databehandleravtale. Databehandleravtalen kan være en frittstående avtale eller den kan være en integrert del av en leveranse- eller tjenesteavtale. Kommunen kan bruke egen mal, eller databehandlerens mal. Databehandleravtalen skal være skriftlig. Det skal fremgå av avtalen at databehandler forplikter seg til å oppfylle lovbestemte krav og kravene i Normen. Databehandler har på lik linje med dataansvarlig et selvstendig ansvar for informasjonssikkerhet og for ivaretakelse av den registrertes personvern.

Les mer om bruk av databehandler i Normens faktaark om databehandlere. Denne inneholder lenke til direktoratet for e-helses mal for databehandleravtaler: https://ehelse.no/normen/faktaark/faktaark-08-avviksbehandling

4.3. Andre aktørers ansvar

Det er vanlig å organisere hele eller deler av anskaffelsen og tjenesteleveransen av velferdsteknologi i fellesskap med flere kommuner. Dette gjøres vanligvis i et Interkommunalt selskap (IKS), vertskommunesamarbeid eller et kommunalt oppgavefelleskap. De utfører et vidt spenn av oppgaver i tilknytning til velferdsteknologi, for eksempel prosjektering, prosjektledelse, utprøving, drift og kontroll. Responssenter er et typisk eksempel på en tjeneste som kommunene drifter i fellesskap. En kommune kan oppnå flere stordriftsfordeler ved å organisere arbeidet med velferdsteknologi på denne måten, i tillegg til å dele på viktig kompetanse.

Kommuner samarbeider ofte om tjenester med andre aktører, som NAV hjelpemiddelsentral, responssenter, spesialisthelsetjenesten, fastleger mv. Dette kan føre til at det er vanskelig å fastsette ansvar, enten det er dataansvar, databehandleransvar, ansvar for utstyret osv. Eksempelvis når kommunen skal følge opp pasient/ bruker som har fått velferdsteknologi levert fra spesialisthelsetjenesten eller NAV hjelpemiddelsentral, er det den virksomheten som anskaffer og leverer ut utstyr til pasient som er ansvarlig for gjennomføring av risikovurderinger og personvernkonsekvensvurderinger. Den virksomheten som følger opp

[12] Les mer om leverandørforhold og avtaler i Normen: https://ehelse.no/normen/normen-for-informasjonssikkerhet-og-personvern-i-helse-og-omsorgssektoren#5.7%20Leverand%C3%B8rforhold%20og%20avtaler

pasient og utstyr og som dokumenterer helse- og omsorgshjelpen i virksomhetens pasientjournal er dataansvarlig for de helse- og personopplysningene som blir behandlet.

5. Sentrale prosesser

Ved både design, anskaffelse, implementering, drift og avvikling er det viktig å involvere de riktige ressursene innenfor personvern og informasjonssikkerhet, slik som personvernombud, juristkompetanse, IKT og sikkerhet, samarbeid med fylkesmannen og å bruke eksisterende nettverk som f.eks andre kommuner i regionen eller Nasjonalt velferdsteknologiprogram.

I designfasen uformes tjenesten med rutiner og retningslinjer. Det er viktig å gjøre en risikovurdering før nye løsninger tas i bruk samt iverksette tiltak for å redusere risiko og personvernkonsekvenser. Les mer om dette i kapittel 5.
.

5.1. Særlig om anskaffelse

Anskaffelser må baseres på behovene til innbyggerne og de ansatte i tjenesten, hvilket krever grundig behovskartlegging før virksomheten lager kravspesifikasjon og går til anskaffelse. Dette er en svært viktig fase for å velge riktig teknologi. Nasjonalt velferdsteknologiprogram har utarbeidet en egen kvikk-guide for anskaffelse i samarbeid med Normen. Det anbefales å lese denne grundig: https://www.ks.no/fagomrader/innovasjon/innovasjonsledelse/veikart-for-tjenesteinnovasjon/kvikk-guide-til-anskaffelser-av-velferdsteknologi/

Leverandører av teknologi til kommuner har ikke et selvstendig ansvar for at teknologien ivaretar kravene i lovverket. Kommunen må derfor stille krav til leverandøren om etterlevelse av regelverk i kravspesifikasjonen, avtaler mv. Normen er et godt hjelpemiddel her. Kommunen kan ta utgangspunkt i oversikt over Normens krav når det utarbeides kravspesifikasjon: https://ehelse.no/normen/oversikt-over-normens-krav-og-mapping-mellom-iso-og-normen

Krav til innebygd personvern bør alltid stilles i kravspesifikasjonen. Det betyr at det skal tas hensyn til personvern og informasjonssikkerhet i alle utviklingsfaser av velferdsteknologien. Forhåndsdefinerte standardinnstillinger bør settes til det mest personvernvennlige nivået.

Når det gjelder kjøp av tjenester vil kravene variere med omfanget av tjenestene. Det vil stilles mer omfattende krav hvis det gjelder kjøp av en hel verdikjede sammenlignet med kjøp av service på utstyr.

Tabellen nedenfor er et forslag til noen punkter i en sjekkliste i anskaffelsesfasen:

1.	Sikre at relevante roller er med i anskaffelsen (f.eks. personvernombud, juridisk, IT, informasjonssikkerhet, helsefag osv.)	☐Ja ☐Nei
2.	Gjennomfør forberedende dialog med leverandør	☐Ja ☐Nei
3.	Framskaff underlag ifm. krav til personvern og informasjonssikkerhet	☐Ja ☐Nei
4.	Ved kjøp av utstyr eller tjeneste bør kommunen utarbeide kravspesifikasjon med utgangspunkt i Normens krav	☐Ja ☐Nei
5.	Still krav til innebygd personvern i produkter og løsninger som anskaffes	☐Ja ☐Nei
6.	Gjennomfør risikovurdering og personvernkonsekvensvurdering av tjenesten/ teknologien	☐Ja ☐Nei
7.	Etabler databehandleravtale dersom leverandør skal behandle helse- og personopplysninger på vegne av kommunen	☐Ja ☐Nei
8.	Fastsette formål med behandlingen og behandlingsgrunnlag	☐Ja ☐Nei

5.2. Særlig om implementering og drift

Når kommunen har valgt teknologi er det viktig å ha gode rutiner for implementering og drift av teknologien.

For implementeringsfasen er det viktig å ha opplæring av brukere og personell, oppdatere styringssystemet for informasjonssikkerhet og personvern, oppdatere oversikten over behandlinger av personopplysninger (protokoll) og etablere tilgangsstyring.
Pasienten/ brukeren skal gis informasjon som er nødvendig for å at pasienten kan samtykke og medvirke til helsehjelpen som ytes. Det betyr at kommunen må gi informasjon om hvordan helsehjelpen gis. I dette må kommunen gi tilstrekkelig informasjon om velferdsteknologien som benyttes i helse- og omsorgshjelpen. Det er viktig at pasienten/ brukeren gis tilstrekkelig opplæring og informasjon om teknologien slik at de ikke bruker denne på feil måter eller til annen bruk enn helse- og omsorgshjelpen. Den informasjonen som gis skal også inkludere behandlingen av helse- og personopplysninger og hva dette omfatter (hva slags personopplysninger, behandlinger og mottakere av opplysningene).

De samme kravene som følger av lov og av Normen gjelder uansett om det er utprøving eller drift. Det er ikke mulig å lempe på tiltakene selv om det er under utprøving av velferdsteknologi. Når det behandles helse- og personopplysninger i utprøvingen skal alle tiltak gjennomføres som om det er normal drift. Dette gjelder uansett om utprøvingen er kortvarig eller går over år.

Når teknologien og/ eller tjenesten er satt i drift skal kommunen alltid følge opp og videreutvikle tjenesten. For arbeidet med informasjonssikkerhet og personvern er det viktig å ha et kontinuerlig fokus.

Tabellen nedenfor er et forslag til noen punkter på en sjekkliste for implementering og drift:

1.	Sikre at relevante roller er med i anskaffelsen (f.eks. personvernombud, juridisk, IT, informasjonssikkerhet, helsefag osv.)	☐Ja ☐Nei
2.	Plasser ansvar og etabler roller	☐Ja ☐Nei
3.	Oppdater styringssystemet for informasjonssikkerhet	☐Ja ☐Nei
4.	Oppdater oversikten over behandling av personopplysninger (protokoll)	☐Ja ☐Nei
5.	Gi informasjon om helse- og omsorgshjelpen som tilbys, teknologien som benyttes og behandlingen av helse- og personopplysninger som vil starte	☐Ja ☐Nei
6.	Gi opplæring til pasient/brukere, pårørende og helsepersonell	
7.	Etabler / vedlikehold tilgangsstyring	☐Ja ☐Nei
8.	Avklar lagringstid for opplysningene og kontinuerlig vurder hva som skal slettes	☐Ja ☐Nei
9.	Gjennomfør logging	☐Ja ☐Nei
10.	Sikre datakommunikasjon	☐Ja ☐Nei
11.	Oppdater konfigurasjonsoversikt ved endringer	☐Ja ☐Nei
12.	Gjennomfør avviksbehandling dersom avvik oppstår	☐Ja ☐Nei
13.	Rydd opp ifm. avvikling hos bruker	☐Ja ☐Nei
14.	Oppdater risikovurdering ved vesentlige endringer, avvik og endringer i risikobilde	☐Ja ☐Nei
15.	Etabler rutine for oppfølging av leverandør (revisjon, avtaler mv)	☐Ja ☐Nei
16.	Etablere rutine for oversikt og vedlikehold av eventuelle samtykker	☐Ja ☐Nei

6. Risiko ved behandling av helse- og personopplysninger i velferdsteknologi

6.1. Risikovurdering

All behandling av helse- og personopplysninger skal risikovurderes. Det er risikovurderingen som ligger til grunn for alle de videre vurderingene og beslutningene; blant annet om man vil ta i bruk en velferdsteknologisk løsning, hvordan behandlingen av opplysningene skal foregå, hvilke tiltak som skal iverksettes, teknisk oppsett av teknologien, hvordan teknologien ivaretar personvernet og informasjonssikkerheten osv.

Alle velferdsteknologiske løsninger som behandler helse- og personopplysninger skal ha "egnede tekniske og organisatoriske sikkerhetstiltak" for å hindre brudd på sikkerheten. Brudd defineres som utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger.

Valg av egnede sikkerhetstiltak skal gjøres på bakgrunn av omfang og kategorier av opplysningene, pasientsikkerhet, aktuelt risikobilde mv. Tiltakene skal velges basert på risikovurderinger, og være forholdsmessige ut fra identifisert risiko.

I arbeidet med risikovurdering er det viktig å ha med ulike typer kompetanse: helsepersonell, juridisk, personvern, informasjonssikkerhet, drift, anskaffelse mm. Dette skal kommunen ha tilgang på.

Det er lurt å bruke kommunens metodikk og malverk. Eksempel på metode for risikovurdering, se faktaark 7 om risikovurdering.

6.2. Brukerscenarier

Se Normens veileder for medisinsk utstyr: https://ehelse.no/normen/veiledere/veileder-i-personvern-og-informasjonssikkerhet-medisinsk-utstyr

6.3. Personvernkonsekvensvurdering i velferdsteknologiske løsninger

Kommunen skal alltid vurdere hvilke konsekvenser behandling av helse- og personopplysninger medfører for den registrerte. Kommunen skal dokumentere lovligheten av behandlingen, formålet, hvordan personvernet til den registrerte er ivaretatt, og at det er gjort tilstrekkelige tiltak for å håndtere risikoen. Hvis det da er sannsynlig at en behandling medfører høy risiko for de registrerte, skal kommunen gjennomføre en mer grundig personvernkonsekvensvurdering, også kalt DPIA.

Bruk av velferdsteknologi i helse og omsorg er en aktivitet som kan medføre høy risiko for de registrertes rettigheter og friheter. Særlig vil følgende aktiviteter i behandling føre til at kommunen må gjennomføre DPIA:

- Systematisk monitorering som innføring av digitalt tilsyn, GPS klokker og annen sporingsteknologi.
- Når helseopplysninger behandles i stor skala
- Ny teknologi
- Barn og andre sårbare grupper

Ikke all velferdsteknologi vil medføre høy risiko for den registrertes rettigheter og friheter. I vurderingen av dette så kan det være aktuelt å vurdere

- omfang av personopplysninger
- personopplysningenes art (hvem opplysningene gjelder, sensitivitet osv.)
- kategorier av mottakere (deling, utlevering, innsyn osv.)
- kategorier av behandlinger (innsamling, sammenstilling, lagring osv.)

Vurderinger av personvernkonsekvenser vil bero på en helhetsvurdering hvor en må ta stilling til kategorier av personopplysninger, behandlinger, mottakere, formålet og sammenhengen opplysningene behandles i. Om kommunen gjør denne helhetsvurderingen basert på punktene over kan kommunene komme frem til gode avgjørelser.

Dersom kommunen kommer frem til at det ikke er behov for å gjennomføre en full DPIA, må dette dokumenteres og være saklig begrunnet.

Løsninger som i utgangspunktet ikke vil være høy risiko for den registrertes rettigheter og friheter:

- Teknologi som ikke behandler helse- og personopplysninger
- Forbrukerteknologi som pasienten/ brukeren selv tar i bruk
- Teknologi som ikke kobles til nettverk
- Stille sykesignalanlegg

Eksempel – elektronisk medisineringsstøtte
Normland kommune skal implementere elektronisk medisineringsstøtte. Medisindispenseren plasseres hjemme hos brukerne hvor et fjernpleiesystem gjør det mulig for ansatte å sjekke om pasienten/brukeren har tatt medisinene som de skal. Normland ønsker å forbedre pasientsikkerheten ved at pasienten/brukeren får rett medisin til rett tid og håper at medisinavvikene går ned.

Normland kommune gjør flere vurderinger (bl.a. risikovurdering, helsefaglige vurderinger) for å sikre at løsningen ivaretar krav til informasjonssikkerhet og personvern. De vurderer konsekvensene for personvernet til pasienten/ brukeren, om de har behandlingsgrunnlag og et klart formål og om det er nødvendig og gjennomføre en DPIA etter personvernforordningen artikkel 35. Kommunen gjennomfører den overordnende vurderingen. De vurderer at:

- innføringen av medisindispenserne ikke er en ny prosess da hjemmetjenesten i mange år har jobbet med medisineringsstøtte. Teknologien settes opp med en integrasjon til EPJ. Prosessen inkluderer ikke bruk av forsystem i en skytjeneste
- løsningen ikke samler inn nye personopplysninger om pasientene enn det de allerede gjør
- personopplysningene som behandles ikke er så omfattende.
- teknologien ikke er ny siden dette er blitt brukt i mange andre kommuner
- leverandør får tilgang til opplysningene som registreres i teknologien
- det behandles helseopplysninger i form av type medisiner som kan avsløre et helseforhold.
- det ikke blir inngripende kontakt mellom tjenesten og pasient/bruker. Dersom pasienten/ brukeren ikke tar medisin som planlagt vil dette følges opp av hjemmetjenesten som normalt.

På bakgrunn av vurderingen inngår de en dekkende databehandleravtale og konkluderer med at det ikke er behov for å gjennomføre en DPIA etter artikkel 35.
De dokumenterer konklusjonene sine.

Det finnes mange ulike verktøy og maler for gjennomføring av DPIA. Direktoratet for e-helse har utarbeidet en mal som kan benyttes for større prosjekter i kommunen.
Bærum kommune har utarbeidet en mal for DPIA som kan benyttes i kommunens arbeid med DPIA.

Besøksadresse
Direktoratet for e-helse
Verkstedveien 1
0277 Oslo

Kontakt
sikkerhetsnormen@ehelse.no