KVIKK-GUIDE TIL BEHANDLING AV HELSE- OG PERSONOPPLYSNINGER
VED BRUK AV VELFERDSTEKNOLOGI

Nasjonalt velferdsteknologiprogram

KS NORMEN Direktoratet for e-helse Helsedirektoratet

Versjon 2 – desember 2019

INTRODUKSJON

Målgruppe
Denne guiden er for dere som arbeider med velferdsteknologi i den kommunale helse- og omsorgstjenesten, og som har fått erfaring og basiskunnskaper på dette området. Det anbefales at man har satt seg inn i Veikart for tjenesteinnovasjon og at man har lest Kvikk-guide til velferdsteknologi.

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

For å sikre dette, må den dataansvarlige (kommunen) sørge for at opplysningene ivaretas, brukes og **behandles på en sikker måte**. Videre må det sørges for at relevant og nødvendig informasjon er tilgjengelig for de som skal ha tilgang til den, og at informasjonen er korrekt. Det må sikres at opplysningene ikke kommer på avveie, og at uvedkommende ikke får tilgang til dem.

Uten betryggende behandling av relevant og nødvendig informasjon, er det ikke mulig å gi helse- og omsorgstjenester av god kvalitet.

Denne guiden tar for seg problemstillinger og temaer innenfor bruk av velferdsteknologi ved ytelse av helse- og omsorgstjenester, spesielt med tanke på **behandling av helse- og personopplysninger.**

Arbeidet med personvern og **informasjonssikkerhet** må være forankret på et tilstrekkelig høyt nivå i organisasjonen. Alle har ansvar for å delta i opplæring og endringsprosesser i virksomheten.

Ved innføring av velferdsteknologi møter mange kommuner utfordringer som berører behandling av helse- og personopplysninger. Selv om behandling og helse- og personopplysninger ikke er nytt innenfor helse- og omsorgstjenesten, kan utfordringene oppleves større og annerledes enn før. Det er flere grunner til dette:

- Bruk av velferdsteknologi genererer mye informasjon om pasienter og brukere, og det må vurderes om 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 behandlingen av opplysningene, 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.

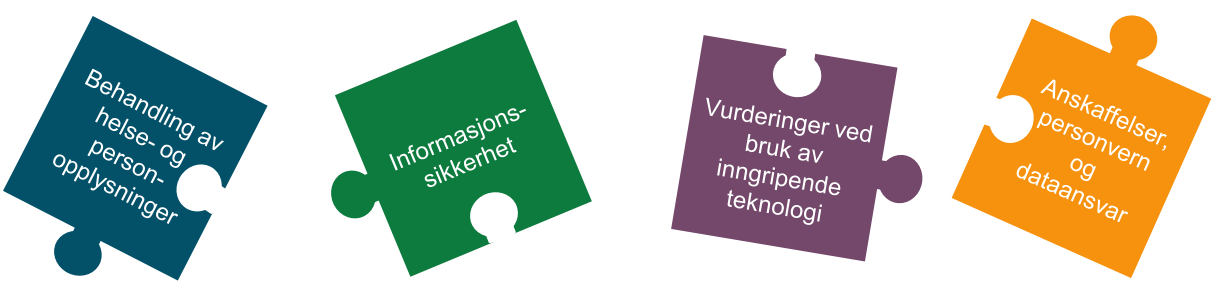
- Ny personopplysningslov, som gjør EUs personvernforordning (GDPR) til norsk lov, har gitt et økt fokus på personvern og reglene for behandling av helse- og personopplysninger. Det har også medført noen nye krav. Forordningen krever bl.a. at det gjøres en personvernkonsekvensutredning (DPIA) når man innfører teknologi som involverer behandling av helse- og personopplysninger. Det skal også føres en skriftlig oversikt (protokoll) over behandling av opplysningene.

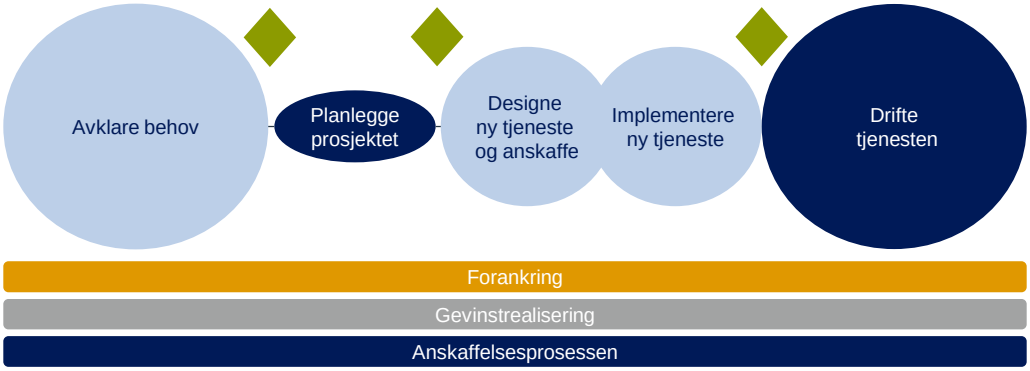
- Flere velferdsteknologiske løsninger gir mulighet for kontroll eller overvåking av brukeren. Dette stiller krav til kunnskap om regelverket rundt bruk av inngripende teknologi.

Hvert kapittel har forslag til vurderinger og verktøy – i samme betydning som verktøy i «Veikart for tjenesteinnovasjon».

Guiden er utviklet av en arbeidsgruppe med medlemmer fra Helsedirektoratet, Direktoratet for e-helse, Normen og PA Consulting

Kvikk-guiden er en hjelp til å ta i bruk velferdsteknologi på en riktig, trygg og sikker måte.





VIKTIGE OPPGAVER I DE ULIKE PROSJEKTFASENE BESKREVET I KVIKK-GUIDE TIL VELFERDSTEKNOLOGI

I «Kvikk-guide til velferdsteknologi» er det beskrevet fem faser for innføring av velferdsteknologi (illustrert i figuren øverst på siden). I dette kapittelet beskrives aktiviteter og vurderinger knyttet til behandling av helse- og personopplysninger i hver av disse fasene.

Avklare behov

I behovsfasen er det viktig å avklare roller og ansvar, for eksempel:

- Er det riktig kompetanse i prosjektet? Hvis ikke må man innhente det, enten fra kommunens egne ressurser eller utenfra.
- Lag oversikt over tjenestens behandling av opplysninger. Hvilke opplysninger skal behandles, og hvem skal behandle opplysningene?

Planlegge prosjektet

Når dere planlegger prosjektet og etablerer prosjekt- og styringsgruppe, er det viktig å involvere riktige ressurser innenfor personvern og informasjonssikkerhet, slik som:

- Personvernombud
- Juristkompetanse
- IT og sikkerhet
- Samarbeid med fylkesmannen
- Eksisterende nettverk, for eksempel andre kommuner i Nasjonalt velferdsteknologiprogram

Designe ny tjeneste

Under designfasen utformes den nye tjenesten med rutiner og retningslinjer. Her er det viktig å tenke på følgende knyttet til behandling av helse- og personopplysninger:

- Gjør en risikovurdering før nye løsninger tas i bruk.
- Gjennomfør personvernkonsekvensvurdering
- Sett i verk tiltak som identifisert i risikovurdering og personvernkonsekvensvurdering
- Beskriv eventuelt behov for innebygd personvern i anskaffelse, konfigurasjon/oppsett og test av nye tekniske løsninger.
- Vurder lagringstid for opplysninger
- Sørg for å ha rutiner for oppfølging av logger

Implementere ny tjeneste

I denne fasen er det fokus på implementeringsplaner og opplæring av brukere og personell. Det handler om å være forberedt på overgang til drift, også med tanke på personvern og informasjonssikkerhet:

- Oppdater styringssystemet for informasjonssikkerhet
- Oppdater oversikt over personopplysninger
- Planlegg og gjennomfør opplæring av brukere og personell
- Etabler tilgangsstyring

Drifte tjenesten

Når ny teknologi og nye tjenester er satt i drift, må man fortsatt følge opp og videreutvikle tjenestene. Dette gjelder ikke minst med tanke på behandling av helse- og personopplysninger:

- Gjennomfør kontinuerlig tiltak for informasjonssikkerhet
  - Sikre datakommunikasjon
  - Oppdater konfigurasjonsoversikten
  - Følg opp logger
  - Vedlikehold tilgangsstyring
- Gjennomfør avviksbehandling
- Gjennomfør oppfølging av leverandør

Verktøy

- E-Helse: Mal for databehandleravtale
- Normen: Veileder i informasjonssikkerhet ved bruk av velferdsteknologi
- Normens faktaark 15: Logging og oppfølging av logger
- Datatilsynet: Risikovurdering av informasjonssystem
- Difi: Informasjonssikkerhet og personvern i IKT-anskaffelser

BEHANDLING AV HELSE- OG PERSONOPPLYSNINGER

Dette kapittelet beskriver hvordan helse- og personopplysninger skal behandles på lovlig måte. Eksempler på personopplysninger er helseopplysninger i journal, registre, fagsystemer, forskning osv. Se blant annet «Viktig om samtykke» i et senere kapittel.

Lovlig behandling
Kommunen skal ha kunnskap om og oversikt over hvilke personopplysninger kommunen behandler, hvorfor de behandles og hvordan.

All behandling av helse- og personopplysninger skal ha et lovlig grunnlag. Personopplysningsloven angir ulike grunnlag for lovlig behandling av helse- og personopplysninger.

Behandlingsgrunnlaget skal identifiseres før behandling av helse- og personopplysningen starter, eller ved endringer i behandlingen. Behandlingsgrunnlaget skal dekke alle behandlingene som utføres; innsamling, registrering, lagring, sletting, utlevering mv.

Når det skal behandles opplysninger som er relevante og nødvendige for ytelse av forsvarlige helse- og omsorgstjenester til den enkelte, er det *«nødvendig for oppfyllelse av en rettslig forpliktelse»* som er det aktuelle behandlingsgrunnlaget.

Dersom velferdsteknologi brukes på andre arenaer enn helse- og omsorgstjenesten, må eventuell sektorlovgivning vurderes.

Innebygd personvern
Nye løsninger som utvikles i helse- og omsorgssektoren skal ha innebygd personvern. Det innebærer at hensynet til personvern skal være ivaretatt i alle ledd av utviklingen og implementeringen av nye løsninger. Dataansvarlig skal sikre innebygd personvern.

Les mer på Datatilsynets sider, og still krav til innebygd personvern i produkter og løsninger.

Andre plikter ved behandling av personopplysninger
Når en databehandler skal håndtere personopplysninger på vegne av dataansvarlig skal det opprettes en databehandleravtale.

Virksomheten skal ha en skriftlig oversikt over behandlingen av personopplysninger – «Protokoll over behandlingsaktiviteter». Dersom virksomheten skal drive forskning, enten alene eller i samarbeid med andre, er det viktig å sette seg inn i regelverket om hvordan helse- og personopplysninger skal behandles for dette formålet. Disse reglene er forskjellige fra regelverket om behandling av opplysninger ved ytelse av helse- og omsorgstjenester. Det er viktig å ha etablert et lovlig grunnlag for å bruke personopplysninger for forskningsformål; dette kan f.eks. være samtykke eller vedtak om dispensasjon fra taushetsplikten.

Vurderinger
- Vet kommunen hvilke personopplysninger som behandles, samt hvordan og hvorfor de behandles?
- Er det opprettet skriftlig oversikt over behandling av personopplysninger?
- Er det lovlig grunnlag for behandlingen av personopplysninger
- Har kommunen rutiner for å oppdage og håndtere avvik?

Verktøy
- Normens faktaark 8: Avviksbehandling
- Normens faktaark 13: Protokoll over behandlinger av helse - og personopplysninger i virksomheten
- Normens veileder for forskning
- Normens veileder for personvern i små helsevirksomheter
- Datatilsynet: Innebygd personvern

INFORMASJONSSIKKERHET

Personopplysningsloven sier at dataansvarlig skal ha "egnede organisatoriske og tekniske 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 kategori av opplysninger, pasientsikkerhet, aktuelt risikobilde mv. Tiltakene skal velges basert på risikovurderinger, og være forholdsmessige ut fra identifisert risiko.

Risikovurdering
Når nye løsninger utvikles og settes i drift er det viktig å få en oversikt over risikobildet og behovet for tiltak. Kommunen må derfor gjennomføre risikovurderinger for å kartlegge sannsynlighet for, og eventuelle konsekvenser av, uønskede hendelser.

Risikovurderingen ligger til grunn for videre vurderinger, tiltak og beslutninger om:
- Hvorvidt en velferdsteknologisk løsning skal tas i bruk
- Hvordan behandling av personopplysninger skal foregå
- Hvilke tiltak som skal settes i verk

Risikovurdering av velferdsteknologi må gjøres ut fra flere aspekter. Her er noen eksempler:

Tilgjengelighet
- Vurdering av teknisk løsning og tilgjengelighet for helse- og personopplysninger
- Vurdering av dekningsgrad av trådløse nettverk
- Vurdering av utsatthet for ødeleggende programvare

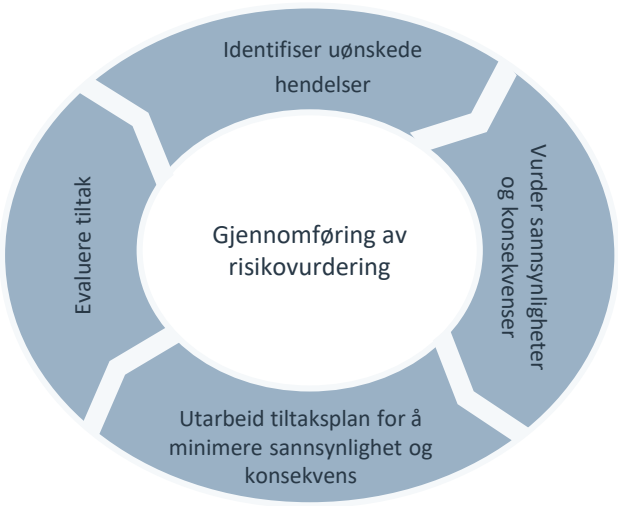
Integritet
- Tilgangsstyring for å hindre utilsiktet endring av helse- og personopplysninger
- Tilstrekkelig opplæring for å hindre brukerfeil
- Annen risiko for ukorrekte helse- og personopplysninger (for eksempel grunnet feil i utstyr og programvare)

Konfidensialitet
- Personopplysninger på avveie
- Løsning for fjernaksess for leverandør
- Bruk av nettbrett (f.eks. eksponering av opplysninger via internettbaserte apper i medisinsk avstandsoppfølging)

Personvernkonsekvensvurdering
Hvis det er sannsynlig at behandling av personopplysninger medfører høy risiko for de registrerte, skal kommunen gjennomføre personvernkonsekvensvurdering, også kalt DPIA. Mer om dette i eget kapittel.

Avviksbehandling
Gjennomføring av risikovurdering og etablering av tiltak vil aldri kunne forebygge alle uønskede hendelser. Uønskede hendelser oppstår, og brudd avdekkes. Når dette skjer skal virksomheten på en systematisk måte registrere, håndtere og følge opp avviket.

Verktøy
- Normens veileder i informasjonssikkerhet ved bruk av velferdsteknologi
- Normens veileder i personvern og informasjonssikkerhet -medisinsk utstyr
- Normens faktaark 7 - Risikovurdering
- Normens faktaark 13 – Protokoll
- Datatilsynets veiledning i informasjonssikkerhet



ANSKAFFELSER, PERSONVERN OG DATAANSVAR

Dialog med leverandører
I forkant av at kravspesifikasjon sendes ut, bør man ha dialog med leverandør som en del av forarbeidet for å spesifisere krav og tiltak knyttet til informasjonssikkerhet.

Krav til leverandører ved kjøp av utstyr respektive tjenester
Leverandører av teknologi til kommunen har ikke 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. Normen er et godt hjelpemiddel her.

Kommunen må videre stille krav til leverandøren om **innebygd personvern.** 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.

Risikovurdering ved anskaffelse
Det skal gjennomføres en fullstendig risikovurdering av det konkrete tilbudet. Risikovurderingen skal gi svar på hvilke tiltak som må eventuelt må iverksettes, og om identifisert risiko kan bli tilstrekkelig redusert med disse tiltakene slik at den kommer innenfor virksomhetens akseptable risiko.

Dataansvarlig og databehandler
Dataansvarlig (i personvernforordningen er dette kalt *behandlingsansvarlig*) er den som bestemmer formålet med behandlingen av opplysningene- og hvilke hjelpemidler som skal brukes. Hjelpemidler her betyr system, metode for lagring og sending osv. Dataansvarlig for behandling av opplysninger i den kommunale helse- og omsorgstjenesten er kommunen.

Databehandler (leverandør, responssenter eller andre) er den som behandler personopplysninger på vegne av den dataansvarlige. Dette forholdet må reguleres i en databehandleravtale.

Når kommunen benytter en leverandør til et oppdrag, vil ikke denne leverandøren nødvendigvis være databehandler. Det er kun når leverandøren 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.

Vurderinger

- Skal det holdes dialog i forkant av anskaffelse?
- Hvilke krav skal stilles til innebygd personvern?
- Skal det opprettes databehandleravtale?

Verktøy

- Mal for databehandleravtale (direktoratet for e-helse)
- Normens veileder i informasjonssikkerhet ved bruk av velferdsteknologi
- Normens veileder i bruk av skytjenester til behandling av helse- og personopplysninger
- Normens Faktaark 6b – Sikkerhetsrevisjon – sjekkliste for å ivareta kravene i Normen
- Normens faktaark 10 – Bruk av databehandler
- Normens faktaark 38 – Sikkerhetskrav for systemer
- Normens faktaark 46 – Dataansvar og avtaler i forbindelse med tjenesteutsetting
- Datatilsynets veileder om behandlingsansvarlig og databehandler
- Datatilsynets veileder for databehandleravtale
- Datatilsynets prinsipper for innebygd personvern
- Kvikk-guide om anskaffelser (kommer)

VURDERINGER VED BRUK AV INNGRIPENDE TEKNOLOGI

Kommunen står langt på vei fritt når det gjelder på hvilken måte den skal oppfylle «sørge for»-ansvaret i helse- og omsorgstjenesteloven § 3-1 første ledd, så lenge de tjenestene som tilbys oppfyller pasientens eller tjenestemottakerens rett til nødvendige og forsvarlige tjenester. Det er i utgangspunktet opp til kommunen å vurdere om et tjenestetilbud skal inneholde velferdsteknologi. Den som mottar tjenestene har imidlertid rett til å medvirke i utformingen av tjenestetilbudet.

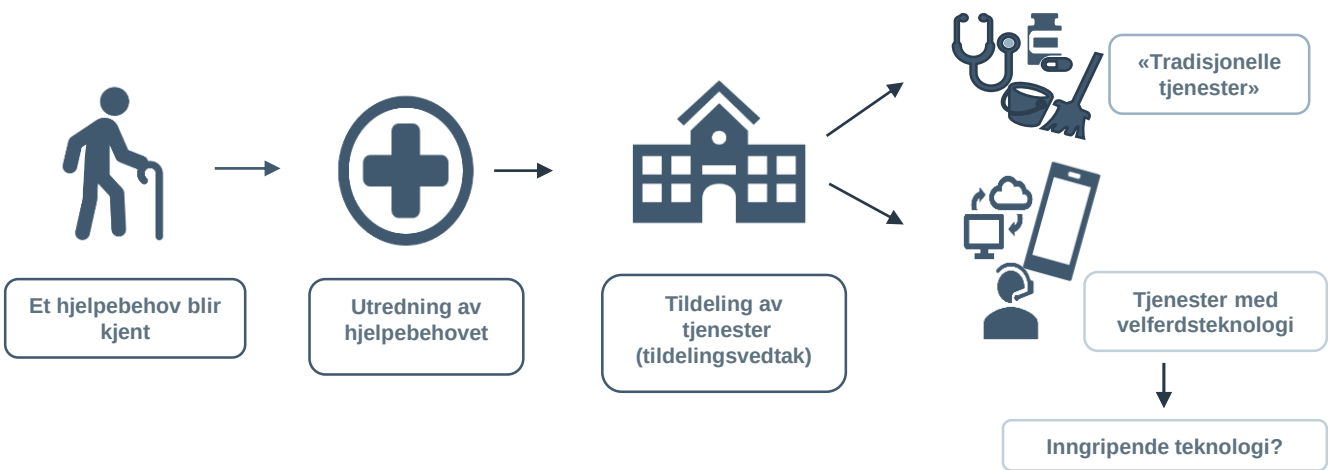
Hvis kommunen kommer til at det er aktuelt å tilby velferdsteknologi, må det vurderes om teknologien er inngripende. Inngripende teknologi er all sporings-, varslings-, lokaliserings- og overvåkningsteknologi som sender informasjon til en tredjeperson om pasientens eller brukerens handlinger, bevegelser, oppholdssted el. uten at pasientens eller brukeren selv initierer det.

Hvis teknologien *ikke* er inngripende, dvs. at den *ikke* sender informasjon om pasienten/brukeren til tredjeperson uten at pasienten/brukeren initierer det selv, er det ikke behov for noe annet rettsgrunnlag enn det – som oftest implisitte – samtykket som ligger til grunn for helsehjelpen/tjenestene, alternativt en beslutning av ansvarlig personell etter reglene i pasient- og brukerrettighetsloven § 4-6 dersom pasienten/brukeren mangler samtykkekompetanse.

Hvis teknologien *er* inngripende, må det vurderes hvilket rettsgrunnlag som er det aktuelle, og om det må fattes vedtak (se *Velferdsteknologiens ABC hefte C, Lovverk og etikk*).

Verktøy

- Helsedirektoratets veileder for saksbehandling av tjenester etter helse- og omsorgstjenesteloven
- Velferdsteknologiens ABC – Lovverk og etikk



VIKTIG OM SAMTYKKE

Rettsgrunnlag for ytelse av helse- og omsorgstjenester

- Samtykke, som oftest implisitt, er grunnlaget for ytelse av helse- og omsorgstjenester til personer med samtykkekompetanse.
- Hvis personen ikke er samtykkekompetent, tas beslutningen om ytelse av helse- og omsorgstjenester av det tjenesteytende personellet, basert på lovhjemmel og/eller ulovfestet rett.
- Ved motstand, psykisk utviklingshemming eller bruk av inngripende teknologi, må vedtak vurderes.

Rettsgrunnlag for behandling av helse- og personopplysninger

- Dokumentasjonsplikten og plikten til bl.a. å sikre forsvarlige tjenester er rettsgrunnlaget for behandling av nødvendige og relevante opplysninger ved ytelse av helse- og omsorgstjenester.
- Behandling av opplysninger utover dette, kan kreve samtykke.

SPØRSMÅL OM SAMTYKKE ER AKTUELT INNEN TO OMRÅDER I HELSE- OG OMSORGSTJENESTEN

1. Ytelse av helse- og omsorgstjenester
Helse- og omsorgstjenester kan i utgangspunktet bare ytes når det tjenestemottakeren samtykker til dette. For helsehjelp følger dette 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:
- En person som gjennom sin atferd viser at han eller hun samarbeider ved ytelse av helse- og omsorgstjenester anses for å ha gitt sitt samtykke (*implisitt samtykke*).
- Samtykket skal likevel være informert, dvs. at personen må ha fått tilstrekkelig informasjon om tilbudet/tjenesten til å vite hva hun eller han "er med på".
- Ved implisitt samtykke er det ikke nødvendig med samtykkeerklæringer som må leses og underskrives

For personer som har samtykkekompetanse, gjelder det ovenstående enten tjenestene ytes med eller uten velferdsteknologi, også inngripende teknologi.

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. Behandling av helse- og personopplysninger
Rettsgrunnlaget for behandling av relevante og nødvendige helse- og personopplysninger i helse- og omsorgstjenesten er dokumentasjonsplikten og plikten til å sikre at de tjenestene som tilbys og ytes er forsvarlige.

Dette betyr:
- Så lenge behandlingen av helse- og personopplysninger er *nødvendig og relevant for tjenesteyting/-administrasjon* skal samtykke ikke benyttes som rettsgrunnlag.
- Behandling av helse- og personopplysninger som nevnt under første kulepunkt for virksomhetsintern kvalitetssikring, krever heller ikke samtykke.

Hvis det skal behandles *flere/andre opplysninger* enn det som er nødvendig og relevant for ytelse og administrasjon av helse- og omsorgstjenester, må nytt behandlingsgrunnlag vurderes. Det kan være at samtykke vil være grunnlag, og da må det innhentes.

Hvis opplysningene skal behandles *for andre formål* enn ytelse og administrasjon av helse- og omsorgstjenester til den enkelte eller intern kvalitetssikring, må også grunnlag for behandling revurderes. Hvis grunnlaget skal være samtykke, må det innhentes. Dette kan for eksempel gjelde hvis opplysningene skal benyttes til forskning.

Verktøy
- Helsepersonelloven – dokumentasjonsplikt
- Velferdsteknologiens ABC – hefte C: Lovverk og etikk
- Veileder for saksbehandling

MER OM PERSONVERNKONSEKVENSVURDERING (DPIA)

Dataansvarlig (kommunen) har plikt til å gjennomføre en vurdering av personvernkonsekvenser før behandling av helse- og personopplysninger starter, når det er sannsynlig at behandlingen vil medføre en høy risiko for fysiske personers rettigheter og friheter (i henhold til artikkel 35 i personvernforordningen, GDPR).

Bruk av velferdsteknologi i helse og omsorg er en aktivitet som kan medføre høy risiko for de registrertes rettigheter og friheter. Man bør spesielt vurdere om aktiviteten innebærer:

- Systematisk monitorering
- Innovativ bruk av teknologiske løsninger
- Opplysninger om sårbare registrerte
- Registrering av sensitive opplysninger

VEILEDNING FOR GJENNOMFØRING AV DPIA

Systematisk beskrivelse av behandlingen

Her går man systematisk til verks og beskriver blant annet:

- Hvilke typer opplysninger samles inn?
- Hvordan foregår innsamlingen?
- Hvem blir registrert, hvor mange og hvor ofte?
- Hva er formålet med registreringen?

Beskrivelsen skal være komplett, tydelig og konkret.

Nødvendighet og proporsjonalitet

Her kvalitetssikrer man at behandlingen av helse- og personopplysninger er nødvendig, at det finnes rettslig grunnlag og at det er samsvar mellom rettsgrunnlaget og formålet med behandlingen av helse- og personopplysninger.

Som ledd i dette må det gjøres en vurdering av rettslig grunnlag/hjemmel, og om formålet er klart definert.

Risiko for de registrertes rettigheter og friheter

I denne fasen skal man gjennomføre en vurdering av personvernkonsekvenser.

Med personvernkonsekvenser menes de konsekvenser den aktuelle behandlingen av helse- og personopplysninger har for den registrertes rettigheter og friheter etter personvernforordningen.

Ledelsens validering av DPIA

I denne fasen har ledelsen eller styret den viktigste rollen, men arbeidet må sammenstilles slik at ledelsen har grunnlag for å gjennomføre en validering. Ledelsen må være bevisst at deres virksomhet behandler personopplysninger som sannsynligvis kan medføre høy risiko for den registrertes rettigheter og friheter.

Presenter tiltak som er valgt for å sikre at dere overholder de grunnleggende prinsippene for etterlevelse av personvernregelverket

Presenter tiltak som er valgt for å gi tilstrekkelig informasjonssikkerhet i henhold til «beste praksis» Kartlegg risikoene ut fra alvorlighetsgrad og sannsynlighet.

Utarbeid en handlingsplan basert på tilleggstiltak som ble identifisert under foregående trinn: for hvert tiltak bestem som et minimum hvem som er ansvarlig for gjennomføring, kostnad (økonomisk eller arbeidsbelastning) og estimert tidsramme.

Verktøy

- KINS mal for gjennomføring av DPIA
- Datatilsynets veileder for DPIA
- Datatilsynets sjekkliste for vurdering av personvernkonsekvenser (DPIA)