HELSEPLATTFORMEN
for pasientens helsetjeneste

Bilag 7 – Behandling av personopplysninger

18. februar 2022

Forhandlet versjon

Innhold

Endringshistorikk

Versjon	Endring	Dato	Ansvarlig

Kvalitetskontroll

Dato	Kontrollert av	Rolle / Funksjon	Status

1 Innledning

Helse- og omsorgsdepartementet (HOD) har med hjemmel i pasientjournalloven § 9 annet ledd [dato] fattet et enkeltvedtak om behandling av personopplysninger i Løsningen ("Enkeltvedtaket"). Enkeltvedtaket fastlegger partenes respektive dataansvar og plikter for oppfyllelse av krav i personvernlovgivningen.

Dette Bilag 7 fastsetter og konkretiserer partenes forpliktelser slik de fremgår av Enkeltvedtaket. Bilaget pålegger også Kunden forpliktelser overfor andre kunder som har signert Tjenesteavtalen. Bilaget oppfyller sammen med Enkeltvedtaket krav om avtale etter pasientjournalloven § 9 første ledd.

Det overordnede formålet med dette bilaget er å sørge for at behandling av personopplysninger i Løsningen skjer på en måte som oppfyller alle lovpålagte krav vedrørende behandling av personopplysninger, herunder særlig at den registrertes personverninteresser blir ivaretatt.

2 Definisjoner

Begreper brukt i dette bilaget som er definert i personvernforordningen artikkel 4 skal forstås i samsvar med nevnte bestemmelse.

«Personvernlovgivningen» inkluderer både generell og sektorspesifikk lovgivning om behandling av personopplysninger, herunder men ikke begrenset til, personopplysningsloven som implementerer EUs personvernforordning og pasientjournalloven med forskrifter.

3 Dataansvar

Helseplattformen og Kunden opptrer som samarbeidende, selvstendige dataansvarlige virksomheter ved oppfyllelsen av de plikter som påhviler partene i medhold av personvernlovgivningen og som nærmere fastsatt i Enkeltvedtaket.

Kunden opptrer også som selvstendig dataansvarlig i relasjon til andre kunder som har signert Avtalen. Det betyr at partene har et selvstendig ansvar for å oppfylle sine forpliktelser slik de fremkommer av Enkeltvedtaket og av dette bilaget.

4 Plikter på informasjonssikkerhetsområdet

4.1 Ansvar for informasjonssikkerhet

Helseplattformen har ansvaret for informasjonssikkerhet i Løsningen. Helseplattformen skal gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen. Tiltakene skal motvirke utilsiktet eller ulovlig tilintetgjøring, tap, endring eller ikke-autorisert utlevering av eller tilgang til helse- og personopplysninger som er overført, lagret eller på annen måte behandlet i Løsningen, jf. pasientjournalloven § 22. Helseplattformen skal for øvrig følge Norm for informasjonssikkerhet i helse- og omsorgssektoren.

4.2 Plikt til å utføre risikovurderinger

Som et ledd i arbeidet med informasjonssikkerhet i Løsningen skal Helseplattformen utføre risikovurderinger. Resultatet av risikovurderinger skal dokumenteres. Kunden skal få tilgang til dokumentasjon fra risikovurderinger.

4.3 Ansvar for sikker autentisering

Helseplattformen skal sørge for sikker autentisering av autoriserte brukere, basert på den autentiseringsmekanismen Kunden har, jf. pasientjournalforskriften § 13 andre ledd. Kundens autentiseringsmekanisme må som et minimum være basert på sikkerhetsnivå 4, med mindre noe annet besluttes.

Partene skal ellers sørge for at autentisering skjer i samsvar med krav oppstilt i Norm for informasjonssikkerhet i helse- og omsorgssektoren.

4.4 Ansvar for autorisasjoner

Helseplattformen skal på bakgrunn av Kundens bestillinger autorisere brukere som skal få tilgang til Løsningen, herunder opprette og vedlikeholde et autorisasjonsregister. Tilgangsstyringen i Løsningen skal følge de til enhver tid vedtatte prinsipper for tilgangsstyring som er besluttet i felles beslutningsstruktur, på signeringstidspunktet inntatt som Underbilag 7.2.

Det er Kunden som er ansvarlig for at informasjonen kun tilfaller personell med tjenstlig behov i sin organisasjon. Dette sikres ved at Kunden er ansvarlig for informasjonsgrunnlaget i sine bestillinger av autorisasjoner, herunder at bestilte autorisasjoner knytter seg til personer som har et tjenstlig behov i kraft av arbeidsoppgavene vedkommende har i virksomheten, jf. pasientjournalforskriften § 13.

4.5 Krav om rutiner for bruk av utstyr mv.

Kunden skal ha interne rutiner for sikker bruk av utstyr som er tilknyttet Løsningen og sikker håndtering av personlig påloggingsinformasjon, jf. pasientjournalloven § 23 og forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten.

4.6 Tilgjengeliggjøring av pasientjournaler for helsepersonell utenfor Helseplattformen

Helseplattformen skal opprettholde full samhandlingsfunksjonalitet med andre aktører, og skal sørge for at relevante og nødvendige opplysninger i pasientjournalen kan gjøres tilgjengelig for helsepersonell utenfor Helseplattformen, jf. pasientjournalloven § 19. Helseplattformen beslutter på hvilken måte opplysningene skal gjøres tilgjengelige og skal sørge for at tilgjengeliggjøring skjer på en sikker måte.

Kunden beslutter i hvilke tilfeller og i hvilket omfang helsepersonell utenfor Helseplattformen skal få tilgang til journalopplysninger fra Løsningen, samt eventuelle tilgangsbegrensninger (for eksempel kun lesetilgang, eller skrivetilgang). Kunden er ansvarlig – både overfor Helseplattformen og øvrige kunder - for at en beslutning om slik tilgang er i tråd med gjeldende regelverk, herunder helsepersonelloven § 25 og § 45.

4.7 Loggføring av journaloppslag og etterfølgende kontroll

Helseplattformen plikter å sørge for at alle oppslag i journalopplysninger loggføres slik at Kunden til enhver tid har mulighet til å se hvem som har gjort oppslag og/eller endringer i en pasientjournal. Loggen skal inneholde all informasjon som foreskrevet i pasientjournalloven § 22 andre ledd og pasientjournalforskriften § 14.

Helseplattformen skal gjøre tilgjengelig et effektivt verktøy for analyse og rapporter til personell Kunden velger, som viser oppslag i pasientjournaler for den Kunden rapporten konkret gjelder. Kunden har selv ansvar for å kontrollere rapporten, og følge opp helsepersonellet og pasientene ved mistanke om snoking (brudd på pasientjournalloven § 16 og helsepersonelloven § 21a).

Helseplattformen og Kunden skal samarbeide med andre kunder med mål om felles læring og utvikling av metodeverk for logganalyse.

Helseplattformen skal følge opp enkeltvedtakets pålegg om å arbeide for at kundene får et verktøy for automatisert logganalyse som forenkler arbeidet med gjennomgang og oppfølging av logger.

4.8 Brudd på personopplysningssikkerhet

Dersom Kunden identifiserer et brudd på personopplysningssikkerheten i Tjenesten (jf. pasientjournalloven § 22, jf. personvernforordningen artikkel 4 nr. 12), skal Kunden omgående varsle om dette via Helseplattformens rapporteringsverktøy. Helseplattformen skal følge opp avviket, herunder om nødvendig eller påkrevet rapportere videre til de andre kundene, tilsynsmyndighetene og de registrerte, jf. personvernforordningen artikkel 33 og 34. Dette gjelder også dersom Helseplattformen selv oppdager avviket.

4.9 Uenighet om informasjonssikkerhet

Dersom Kunden og Helseplattformen er uenige om informasjonssikkerhetsrisiko knyttet til Løsningen eller egnede tiltak for å håndtere slik risiko, skal partene drøfte risiko og eventuelle tiltak med den hensikt å oppnå en omforent forståelse av krav til informasjonssikkerhet.

Dersom Kunden og Helseplattformen ikke oppnår enighet, skal problemstillingen løftes opp til diskusjon i det organ Kunden har utpekt for dette formålet. [For kunder i Helse Midt-Norge RHF er Regionalt informasjonssikkerhetsforum (RIF) utpekt som eskaleringsnivå ved uenighet]. Dersom Kunden ikke utpeker noe slikt organ løftes uenighet til Faglig beslutningsstruktur (Fagteam data/IKT). Dersom uenigheten knytter seg til forhold som også har betydning for andre kunder skal Helseplattformen parallelt med at saken løftes til organet utpekt av Kunden, ta opp saken i Faglig beslutningsstruktur (Fagteam data/IKT).

Helseplattformen skal legge vekt på oppfatninger som fremlegges av Kunden og andre kunder vedrørende problemstillingen det er uenighet om.

Partene skal ta i bruk øvrige mekanismer for å løse uenighet i Tjenesteavtalen med bilag først når drøfting og diskusjon i ovennevnte organer er gjennomført, i samsvar avsnitt 1- 3 over. Der Helseplattformen er ansvarlig for informasjonssikkerheten i Løsningen, der det ikke er praktisk mulig å innhente synspunkter i forkant av at egnede tiltak må settes inn mot en identifisert risiko, skal Helseplattformen umiddelbart gi varsel til Kunden om at tiltak vil iverksettes, og i etterkant av tiltaket legge saken frem til drøfting i ovennevnte fora med en begrunnelse for

hvorfor det ikke var mulig å avvente tiltaket. Kunden har rett til å be om at ovennevnte varsel alternativt eller i tillegg gis til en utpekt systemeier i virksomheten.

4.10 Etablering av felles faglig forum

Det skal opprettes et faglig forum for å diskutere og gi råd i saker som gjelder informasjonssikkerhet, tilgangsstyring og personvern. Helseplattformen skal være fast representert i forumet. Kundens deltakelse er frivillig, men det skal tilstrebes å ha deltakelse fra et representativt utvalg.

5 Plikter overfor de registrerte

5.1 Informasjon og innsyn

Helseplattformen skal utarbeide generell informasjon om behandlingen av helse- og personopplysninger i Helseplattformen, jf. personvernforordningen artikkel 13 og 14.

Kunden skal informere sine pasienter om at Kunden bruker Løsningen, herunder hva det innebærer for pasientene. Kunden skal for øvrig henvise til informasjonen som er utarbeidet av Helseplattformen.

Kunden har et selvstendig ansvar for å oppfylle informasjonsplikten ovenfor pasientene knyttet til behandling av personopplysninger som ikke er en del av Tjenestene.

Helseplattformen skal gjennom helsenorge.no og via pasientportalen i Løsningen tilrettelegge for at registrerte enkelt kan få innsyn i opplysninger om seg selv, herunder innsynslogger, jf. pasient- og brukerrettighetsloven § 5-1, helsepersonelloven § 41, pasientjournalloven § 18 og pasientjournalforskriften § 14.

Dersom pasienten (eller andre som har rett til innsyn) velger å kontakte Kunden i stedet for å bruke helsenorge.no eller pasientportalen i Løsningen, skal Kunden gi pasienten innsyn i pasientjournal eller andre aktuelle opplysninger.

5.2 Retting, sletting og sperring av journalopplysninger

Kunden er kontaktpunkt for pasientene sine og er ansvarlig for å behandle henvendelser som forutsetter helsefaglige vurderinger. Dersom Kunden mottar en forespørsel om retting, sletting eller sperring av journal skal Kunden vurdere, eventuelt i samarbeid med andre berørte kunder, om det er grunnlag for å foreta retting, sletting eller sperring av journalen, jf. helsepersonelloven §§ 42-44, pasient- og brukerrettighetsloven § 5- 2 og pasientjournalforskriften § 15.

Helseplattformen skal yte bistand til Kunden med å oppfylle nevnte forpliktelser overfor de registrerte. Helseplattformen skal bistå Kunden med å effektuere en beslutning om retting, sletting eller sperring av journal.

5.3 Øvrige plikter overfor de registrerte

Utover de forhold som er nevnt i punktene 5.1 og 5.2, har Kunden og Helseplattformen ansvar for plikter og rettigheter for pasienter i samsvar med bestemmelser i lov eller forskrift.

6 Internkontroll og dokumentasjonsforpliktelser

6.1 Oversikt over behandlinger

Helseplattformen skal utarbeide og vedlikeholde en protokoll over behandling av helse- og personopplysninger om pasienter (og eventuelle representanter), jf. personvernforordningen artikkel 30 nr. 1. Helseplattformen skal også utarbeide og vedlikeholde en protokoll over behandling av personopplysninger om autoriserte brukere av Helseplattformen. Protokollene skal på egnet måte gjøres tilgjengelig for Kunden.

Kunden skal orientere seg om de protokollene som er utarbeidet og har ansvar for å supplere de protokollene dersom Kunden behandler personopplysninger for andre formål eller på en annen måte enn beskrevet i nevnte protokoller. Kunden kan bruke informasjon fra Helseplattformens protokoll til å utforme sine egne protokoller. Dersom Kunden mener det er feil eller mangler ved Helseplattformens protokoller, skal Kunden varsle Helseplattformen om dette.

6.2 Personvernkonsekvenser

Helseplattformen er i Enkeltvedtaket pålagt et ansvar for å vurdere personvernkonsekvenser forbundet med behandling av helse- og personopplysninger i Løsningen, jf. personvernforordningen artikkel 35. Helseplattformen skal orientere Kunden om resultatene av slike vurderinger.

Helseplattformen er ansvarlig for å ivareta krav om å vurdere og eventuelt gjennomføre forhåndsdrøftinger etter GDPR art 36.

Kunden vurderer på hvilken måte man skal følge opp og implementere tiltak som besluttes på bakgrunn av vurderingene.

Kunden må gjøre egne vurderinger av personvernkonsekvenser når det gjelder behandlinger som ikke er en del av Tjenestene.

6.3 Plikt til egenrevisjon

Kunden skal jevnlig revidere sin egen bruk av Helseplattformen, herunder særlig kontrollere rutiner vedrørende egne ansattes autorisasjoner, jf. pasientjournalloven § 23 og forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten. Brudd på personopplysningssikkerheten skal varsles til Helseplattformen, jf. pkt. 4.7.

Helseplattformen skal revidere løsningen minst i den grad det er nødvendig for å sikre tilstrekkelig informasjonssikkerhet i samsvar med punkt 4 over. Dokumentasjon og vurderinger utformet i forbindelse med revisjoner, skal gjøres tilgjengelig for kunder, med mindre taushetsplikt eller vern av forretningshemmeligheter tilsier hemmelighold.

6.4 Landrisiko

Som del av risikovurderinger skal Helseplattformen, før opplysninger legges hos databehandler utenfor Norge, også innen EU/EØS, gjennomføre landrisikovurderinger iht. enhver tid beste praksis. Kunden skal gjøres kjent med vurderingskriteriene som anvendes.

7 Oppfølging av databehandlere mv.

7.1 Inngåelse og forvaltning av databehandleravtaler

Helseplattformen har ansvaret for at det foreligger gyldige databehandleravtaler med alle databehandlere som deltar ved leveransen av Tjenestene, og for forvaltning av slike avtaler. Helseplattformen skal i nødvendig utstrekning gjøre revisjoner av databehandlere for å sikre forsvarlige og sikre leveranser til Kunden.

7.2 Overføringsgrunnlag

Helseplattformen har ansvar for at det foreligger et gyldig overføringsgrunnlag ved behandling av personopplysninger utenfor EØS-området, der behandlingen av personopplysninger er en del av Tjenestene.

Helseplattformen skal overfor Kunden gjøre tilgjengelig sine vurderinger knyttet til hvorvidt personopplysninger som blir overført får tilstrekkelig beskyttelsesnivå på lik linje som i EU/EØS før overføringen.

8 Bruk av helse- og personopplysninger til andre formål enn helsehjelp

8.1 Bruk av helse- og personopplysninger til forskning mv.

Kunden har det rettslige ansvaret for og beslutter om og hvordan helse- og personopplysninger i Løsningen skal brukes til andre formål enn helsehjelp, administrasjon og kvalitetssikring av helsehjelpen, jf. pasientjournalloven § 3. Adgangen til å beslutte uttrekk av data er begrenset til opplysninger Kunden selv har nedtegnet for pasienter man har hatt en behandlingsrelasjon til. Kunden er ansvarlig for vurderinger knyttet til hjemmelsgrunnlaget for uttrekk for bruk til andre formål, herunder at det gjennom samtykke eller annet rettslig grunnlag foreligger hjemmel til å gjøre uttrekk av opplysninger nedtegnet av andre dataansvarlige virksomheter. Det skal foreligge skriftlige prosedyrer om beslutningskompetanse hos Kunden for bruk av helse- og personopplysninger til slike sekundære formål.

Kundene skal samarbeide om å koordinere henvendelser om sekundærbruk slik at det oppnås en fullt ut forsvarlig håndtering av slike henvendelser, særlig med tanke på å etablere prosedyrer mellom kundene til som regulerer behandling og vurdering av henvendelser som angår opplysninger nedtegnet av flere dataansvarlige virksomheter. Kundene kan velge å la seg representere at en felles enhet for mottak av henvendelser.

Helseplattformen skal bistå Kunden med uttrekk, sammenstilling og overføring av helse- og personopplysninger til sekundære formål og er ansvarlig for at informasjonssikkerheten ivaretas i den forbindelse. En Kunde som anmoder om uttrekk til sekundærbruk skal fremlegge en redegjørelse for hvilket hjemmelsgrunnlag som anvendes og at vilkår for uttrekk er oppfylt. Helseplattformen skal kun effektuere forespørsler som kommer fra avsender som har formell beslutningskompetanse.

9 Oppbevaring av pasientjournaler

9.1 Oppbevaring av pasientjournaler

Helseplattformen skal sørge for at pasientjournaler i Helseplattformen og tilhørende logger oppbevares til Kunden beslutter at det ikke lenger antas å bli bruk for dem, jf. pasientjournalloven § 25. Helseplattformen skal, i samsvar med Bilag 8, ta stilling til om opplysningene deretter skal bevares etter arkivloven eller annen lovgivning.

9.2 Arkivansvar

Helseplattformen er ansvarlig for oppfyllelse av arkivansvaret for pasientjournaler og annet arkivverdig materiale i Løsningen, jf. arkivlova § 6.

10 Avsluttende bestemmelser

10.1 Forpliktelser ved fratredelse

Dersom en Kunde velger å si opp Avtalen, skal Kunden få utlevert en kopi av relevante og nødvendige opplysninger fra journalen for overføring til Kundens nye journalsystem.

Journalopplysninger som er relevante og nødvendige for gjenværende virksomheter forblir i Løsningen. Resten slettes.

10.2 Endringer i dette bilaget som følge av Enkeltvedtaket

Dersom innholdet i det fastsatte Enkeltvedtaket eller Tjenesteavtalen for øvrig tilsier at dette Bilag 7 må endres, skal Kunden og Helseplattformen drøfte og foreta justeringer/oppdateringer av bilaget med den hensikt å utforme nye formuleringer i samsvar med Enkeltvedtaket. Partene skal forsøke å oppnå enighet om formuleringene.

Underbilag 7.1 – Varsel om vedtak – Helseplattformen og dataansvar[1]

Underbilag 7.2 - Prinsipper for tilgangsstyring i Helseplattformen v.1.0

[1] Brev fra Helse- og omsorgsdepartementet (HOD) datert 10. februar 2022, HOD referanse 20/2985-3