Ahus - Utarbeidelse, saksbehandling og arkivering av databehandleravtaler

Dokumentadministrator: Renate Brandvoll Johnsen | Gyldig fra: 12.02.2021 | Revisjon: 1.1
Godkjent av: Øystein Mæland | Revisjonsfrist: 12.02.2023 | ID: 39098

1.0 Hensikt

Hensikten med denne prosedyren er å sikre utarbeidelse, saksbehandling og arkivering databehandleravtale når helse- og personopplysninger behandles (eks. lagring, backup, sletting eller endring) av ekstern part.

2.0 Omfang

Gjelder for systemeiere, systemansvarlige og andre som forvalter IKT-systemer, Medisinsk teknisk utstyr (MTU), samt andre som inngår samarbeidsavtaler, hvor helse- og personopplysninger behandles av ekstern part.

Gjelder også for eksterne parter og leverandører av MTU som skal behandle helse- og personopplysninger.

Gjelder ikke når eksterne parter og leverandører av MTU utfører vedlikehold uten behandling av personopplysninger.

Gjelder ikke dersom taushetsbelagte opplysninger gis til samarbeidende personell når dette er nødvendig for å kunne gi forsvarlig helsehjelp, med mindre pasienten motsetter seg det, jf. Lov om helsepersonell m.v. (helsepersonelloven) §25.

3.0 Arbeidsbeskrivelse

3.1 Ansvar

- **Administrerende direktør:** Er dataansvarlig og har ansvaret for at lagring og forvaltning av helse- og personopplysninger gjøres med nødvendig sikkerhet og kun i samsvar med gyldig behandlingsgrunnlag.
- **Informasjonssikkerhetsleder:** Har det utøvende ansvar for virksomhetens informasjonssikkerhetsarbeid, blant annet ved å godkjenne risikovurderinger og utføre internkontroll med informasjonssikkerheten i virksomheten.
- **Personvernombudet:** Personvernombudet har en rådgivende og kontrollerende funksjon i virksomheten, jf. GDPR artikkel 39.
- **Sykehuspartner:** Har ansvar for å inngå databehandleravtale med sine underleverandører og innleide som har tilgang til personopplysninger.
- **Ledere innen ulike enheter og områder:** Har ansvar for å påse at denne prosedyren implementeres og etterleves innen eget ansvarsområde. Ledere skal også påse at det inngås databehandleravtale ved behov.
- **Systemeier:** Skal signere databehandleravtale i henhold til fullmakter ved Ahus.
- **Systemansvarlig:** Skal påse at det oppdretts sak i saksbehandlingssystemet Public 360, og inngås Databehandleravtale ved behov, samt å arkivere relevant dokumentasjon. Skal også være kontakt punkt mot informasjonssikkerhetsleder og Sykehuspartner.
- **Den som er ansvarlig for MTU:** Har de samme ansvarsområdene som systemansvarlig, men for MTU. I tillegg skal sette inn lenke i Medusa til signert databehandleravtale arkivert i Public 360.
- **Alle ansatte og innleide** som skal lagre og behandle helse- og personopplysninger, skal forholde seg til denne prosedyren. Dette gjelder uavhengig av organisatorisk plassering og yrkesgruppe.

3.2 Handling

Helse Sør-Øst sine krav til bruk av databehandler er beskrevet i EQS 33714 Helse Sør Øst - Bruk av databehandler - Behandling av personopplysninger hos annen juridisk enhet. Databehandleravtale for Ahus finnes på norsk og engelsk i denne prosedyren.

Ved anskaffelser, endringer i tjenester, inngåelse av samarbeidsavtaler, eller ved vedlikehold og reparasjon av MTU, der eksterne parter og leverandører behandler helse- og personopplysninger, skal det opprettes databehandleravtale. Dette gjelder om ekstern part ikke har allerede signert relevant databehandleravtale med Ahus eller Sykehuspartner.

Ved behov for juridisk bistand ta kontakt med jurister ved Ahus.

For IKT-systemer: Systemansvarlig har ansvar for kommunikasjon med Sykehuspartner og klargjøre om databehandleravtale er signert. Om det ikke er undertegnet en slik avtale tidligere, skal systemansvarlig informere systemeier og ta initiativ til å inngå ny databehandleravtale mellom Ahus og leverandør i samråd med systemeier.

Systemeier skal i samråd med informasjonssikkerhetsleder avgjøre om Ahus eller Sykehuspartner skal inngå avtalen.

Databehandleravtale signeres i henhold til kap. 3.3.6 «Informasjonssikkerhet» i Ahus - Fullmakter ved Akershus Universitetssykehus.

For MTU: Den som er ansvarlig for MTU i DDT-MTE-MT har ansvar for kommunikasjon med Sykehuspartner og klargjøre om databehandleravtale er signert. Om det ikke er undertegnet en slik avtale tidligere, skal den ansvarlige ta initiativ til å inngå ny databehandleravtale mellom Ahus og leverandør. Divisjonsdirektør i DDT skal i samråd med informasjonssikkerhetsleder avgjøre om Ahus eller Sykehuspartner skal inngå avtalen.

Databehandleravtale signeres i henhold til kap. 3.3.6 «Informasjonssikkerhet» i Ahus - Fullmakter ved Akershus Universitetssykehus.

Derom ekstern part og leverandør av MTU utfører vedlikehold uten behandling av helse- og personopplysninger, men har tilgang til disse opplysningene, gjelder kun signering av taushetserklæring i henhold til avtale med Ahus.

Saksbehandling og arkivering:

Databehandleravtale skal utarbeides ved bruk av malene som er vedlagt i EQS 33714 Helse Sør Øst - Bruk av databehandler - Behandling av personopplysninger hos annen juridisk enhet.

Saksbehandlingssystemet Public 360 skal benyttes til opprettelse, behandling og arkivering av alle databehandleravtale. Søk i relevante saker kan gjøres i Public 360.

Utarbeidet databehandleravtale skal arkiveres i saker for leverandør (en sak per leverandør som inneholder for eksempel avtaler mm.). Saken skal navngis etter følgende navneregel i Public 360:

Databehandleravtale mellom Ahus og <Leverandør>, fra År(åååå)

Eksempel: Databehandleravtale mellom Ahus og Firma AS, fra 2020

Utarbeidet databehandleravtale (og evt følgebrev/e-post) skal arkiveres (under relevant sak) med følgende navneregel, før den sendes til godkjenning/signering i Public 360:

Databehandleravtale mellom Ahus og <Leverandør> for <Tjeneste/System> fra År(åååå) - Til signering

Eksempel: Databehandleravtale mellom Ahus og Firma AS for System X fra 2020 – Til signering.

Signert databehandleravtale sendes da som vedlegg i e-post (eller papir) til leverandør til signering. Dette skal arkivers i saken som utgående dokument.

Mottatt e-post/brev med vedlagt signert databehandleravtale skal navngis etter følgende navneregel, og arkiveres som inngående dokument i saken:

Databehandleravtale mellom Ahus og <Leverandør> for <Tjeneste/System> fra År(åååå) - Signert

Eksempel: Databehandleravtale mellom Ahus og Firma AS for System X fra 2020 – Signert

Ved behov se Ahus - Public 360 - Generell rutine for elektronisk saksbehandling og sakarkiv.

For MTU og MTU-applikasjoner: I Medusa skal det settes lenke til signert databehandleravtale arkivert i Public 360.

4.0 Relaterte dokumenter

Se relaterte dokumenter.

5.0 Vedlegg

Mal for databehandleravtale finnes som vedlegg i Helse Sør Øst - Bruk av databehandler - Behandling av personopplysninger hos annen juridisk enhet:

Databehandleravtale for Ahus (norsk)

Data processing agreement (engelsk)

6.0 Grunnlagsinformasjon

6.1 Grunnlagsdokumenter

Lov om behandling av personopplysninger (personopplysningsloven)

Personvernforordningen på engelsk - General Data Protection Regulation - GDPR

Helse Sør Øst - Bruk av databehandler - Behandling av personopplysninger hos annen juridisk enhet

6.2 Definisjoner

MTU: Ethvert medisinsk utstyr, inklusiv in vitro-diagnostisk medisinsk utstyr, inkludert programvare og systemløsninger, beregnet for mennesker til diagnose, overvåkning og/ eller behandling på medisinsk grunnlag og som for å fungere er avhengig av en energikilde (strøm, lys, gass- eller væsketrykk) samt nødvendig tilbehør til slikt utstyr.

Systemløsninger: Med systemløsninger forstås medisinsk-teknisk utstyr som virker sammen med IKT-produkter/systemer, der tilsiktet anvendelse (jfr. MDR - Medical Device Regulation) er diagnose, overvåkning og/ eller behandling av mennesker på medisinsk grunnlag. Kommunikasjonen skjer via nettverk, mellom serversystemer, databaser og/eller andre lagringsmedia

For flere definisjoner vennligst se EQS 33688 Ahus - Styrende - Kilder og definisjoner i regionalt styringssystem for informasjonssikkerhet.

7.0 Søkeord

Databehandler, databehandleravtale, DPIA, personvern, personvernkonsekvens, informasjonssikkerhet, MTU, Systemløsninger.

Relaterte dokumenter:

Ahus - Endringskontroll for IKT-applikasjoner, tjenester og medisinsk teknisk utstyr med integrert IKT-styringssystem

Ahus - Fullmakter ved Akershus Universitetssykehus

Ahus - Public 360 - Generell rutine for elektronisk saksbehandling og sakarkiv

DDT - Samarbeidsavtaler

Helse Sør Øst - Bruk av databehandler - Behandling av personopplysninger hos annen juridisk enhet

LAB. AVD. - Endringskontroll og bruk av fleksibel akkreditering

Relaterte lenker:

- Lov om behandling av personopplysninger (Personopplysningsloven)
- Personvernforordningen på engelsk - General Data Protection Regulation - GDPR