



DATABEHANDLERAFTALE

Mellem parterne:

Den dataansvarlige myndighed

Region Nordjylland

Niels Bohrs Vej 30

9220 Aalborg Øst

CVR.nr.: 29 19 09 41

(herefter ”Dataansvarlig”)

og

Databehandler

Copenhagen Trial Unit

Dept. 7812, Rigshospitalet

Tagensvej 22

2100 København

CVR.nr.: 34177058

(herefter ”Databehandler”)

Denne databehandleraftale knytter sig til indgået aftale mellem Region Nordjylland (Anæstesi og Intensiv afdeling, Klinik Akut, Aalborg Universitetshospital) og databehandleren af 22.03.2017

vedrørende

Handling Oxygenation Targets in the Intensive Care Unit, HOT-ICU

hvor data opbevares

Copenhagen Trial Unit (CTU) fysisk placering af data/servere

om

sikkerhedsforanstaltninger i medfør af § 42, stk. 2, jf. § 41, stk. 3-5 i lov nr. 429 af 31.maj 2000 om behandling af personoplysninger **med senere ændringer** (Persondataloven)



1. Databehandlers ansvar

Databehandleren handler alene efter instruks fra den dataansvarlige.

Databehandleren forpligter sig til, til enhver tid at overholde lovgivningsmæssige krav i forbindelse med den databehandling, som udføres for den dataansvarlige.

2. Databehandlers opgave

CTU varetager produktion af og hosting af database og data indhentet i f.b.m.HOT-ICU forsøget herunder eCRF udvikling endvidere forberedelse af database til statistisk analyse

3. Brug af ekstern Databehandler eller underleverandør

Såfremt Databehandleren samarbejder med en underleverandør, skal dette oplyses til den Dataansvarlige, og det er Databehandlerens ansvar at sikre sig at underleverandøren lever op til de krav, den Dataansvarlige har stillet til sikker opbevaring og håndtering af data. Ved indgåelse af aftale med ny underleverandør / skift af eksisterende underleverandør skal den Dataansvarlige adviseres herom min. 1 måned før.

4. Lovbestemmelser

Databehandlingen foregår i henhold til Persondataloven og Justitsministeriets bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, der behandles for den offentlige forvaltning med senere ændringer (sikkerhedsbekendtgørelsen).

Principperne og anbefalingerne i DS484:2005 / ISO 27001 med senere ændringer vil på alle relevante områder finde anvendelse i det omfang andet ikke fremgår af nærværende databehandleraftale.	Ja <input type="checkbox"/>	Nej <input checked="" type="checkbox"/>
--	--------------------------------	--

De nævnte bestemmelser indeholder blandt andet regler om fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med Persondataloven.

5. Tekniske og organisatoriske sikkerhedsforanstaltninger

Databehandleren skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med Persondataloven.

Såfremt der er tale om et system som:

1. indeholder personhenførbare data
2. skal tilgås og transmitteres over internettet

skal Databehandler årligt dokumentere sikkerheden f.eks. gennem en penetrationstest.

6. Ad hoc arbejdspladser

Hvis databehandleren har behov for, at foretage databehandling fra ad hoc arbejdspladser (fjernarbejdspladser eller hjemmearbejdspladser), skal det ske på en måde, som overholder de generelle krav til sikkerhedsforanstaltninger, jf. pkt. 4 og 5.

7. Audit og Revisionserklæring

Databehandleren skal på den Dataansvarliges anmodning give den Dataansvarlige tilstrækkelige oplysninger til at denne kan påse, at de nævnte tekniske og organisatoriske sikkerhedsforanstaltninger er truffet. Endvidere skal Databehandleren kunne dokumentere, at identificerede sårbarheder bliver imødegået ud fra en risikobaseret vurdering.

Da den Dataansvarlige har pligt til aktivt at sikre, at de krævede sikkerhedsforanstaltninger overholdes hos Databehandleren, kan der indgås en gensidig aftale om, at der enten indhentes en årlig revisionserklæring fra en uafhængig tredjepart, eller at den Dataansvarlige kan vælge mellem selv at udføre regelmæssige sikkerhedsaudits, eller kan anmode om tilvejebringelse af dokumentation for at sikkerhedsmæssige foranstaltninger er gennemførte hos leverandøren.

I tilfælde af, at den Dataansvarlige og/eller relevante offentlige myndigheder, særligt Datatilsynet, ønsker at foretage en fysisk inspektion af de ovennævnte foranstaltninger, forpligter Databehandleren sig til – med et rimeligt varsel – at stille tid og ressourcer til rådighed herfor. Den Dataansvarlige kan gennemføre en årlig fysisk inspektion.

8. Underretningspligt

Databehandleren er forpligtet til at underrette den Dataansvarlige skriftligt ved kendskab til enhver afvigelse i forhold til aftalens indhold, f.eks.:

- Ved enhver fravigelse fra givne instrukser
- Ved afvigelse fra det aftalte om tilgængelighed
- Ved planlagte releases, opgraderinger, tests m.v.
- Ved enhver mistanke om brud på fortroligheden
- Ved enhver mistanke om misbrug, fortabelse og forringelse af data

Ved enhver mistanke om alvorlig misligholdelse af aftalen skal den Dataansvarlige endvidere straks underrettes.

9. Håndtering af data efter aftalens ophør

Databehandleren forpligter sig at sikre, at personhenførbare data slettes når databehandlingen jf. aftale med den Dataansvarlige skal ophøre. Det påhviler den Dataansvarlige at oplyse Databehandleren om det tidspunkt, hvor databehandlingen skal ophøre. Det påhviler herefter Databehandleren at slette personhenførbare data ved det oplyste tidspunkt. Sletning må dog ikke ske før Databehandleren har oplyst den Dataansvarlige om den påtænkte fremgangsmåde for sletning og indhentet særskilt bekræftelse fra den Dataansvarlige på at sletning skal gennemføres på den oplyste dato.

Såfremt den Dataansvarlige ikke finder metoden tilstrækkelig effektiv, skal den Dataansvarlige meddele Databehandleren hvilken metode, der anses for tilstrækkelig effektiv.

Ved anmodning fra den Dataansvarlige, skal Databehandleren fremsende en skriftlig erklæring på at data er slettet som aftalt, inklusiv en beskrivelse af den anvendte metode.

10. Aftalens ikrafttræden og varighed

Databehandleraftalen indgås ved begge parter underskrivelse og kan tidligst opsiges af Databehandleren til det tidspunkt hvor databehandlingen jf. aftale med den Dataansvarlige skal ophøre og den i pkt. 9 beskrevne dokumentation er modtaget og accepteret af den dataansvarlige.

Såfremt den Dataansvarlige ikke i tilhørende kontrakt eller efter Databehandlerens gentagne anmodninger har oplyst Databehandleren om det tidspunkt, hvor databehandlingen skal ophøre, er Databehandleren berettiget til ved skriftlig meddelelse til den Dataansvarlige at opsige databehandleraftalen med 3 måneders varsel.



Regionernes
Sundheds-it

Side 5 af 5

Aalborg, den 22.03.2017

For Region Nordjylland:

Navn: Bodil Steen Rasmussen

Titel: Professor, overlæge

Professor, overlæge, ph.d.

Bodil Steen Rasmussen

Klinik Akut

Anæstesi og Intensiv Afdeling
Aalborg Universitetshospital

København, den 22.03.2017

For CTU:

Navn: Jørn Wetterslev

Titel: Overlæge, ph.d.

Copenhagen Trial Unit (CTU)

Jørn Wetterslev

Overlæge, Ph.D.

Rigshospitalet, Dept. 7812
Blegdamsvej 9, DK-2100 Copenhagen Ø
Tel. +45 3545 7159 - Fax +45 3545 7101
E-mail: wetterslev@ctu.dk