Sørlandet sykehus HF | **Databehandleravtale**

Databehandleravtale mellom ……, v/……, og Sørlandet Sykehus HF (org nr. 983 975 240)

1 Kontraktens parter

Kontrakten inngås mellom Databehandlingsansvarlig Sørlandet Sykehus HF (heretter kalt Databehandlingsansvarlig) og Intuitive Surgical Sàrl (heretter kalt Databehandler).

2 Formål og virkeområde for avtalen

Formålet med kontrakten er å regulere Databehandlerens bruk og sikring av personopplysninger som er tilgjengeliggjort av Databehandlingsansvarlig. Det skal fremgå klart dersom Databehandleren kan overlate personopplysninger til andre for oppbevaring, bearbeiding eller annen bruk.

Kontrakten er utformet for å nærmere regulere ansvaret mellom Databehandlingsansvarlig og Databehandleren ved databehandlers drift, forvaltning, bruk og tilgang til helse- og personopplysninger.

3 Varighet og oppsigelse

Avtalen trer i kraft 01.01.2013 og har en varighet tilsvarende utstyrets levetid. Kontrakten kan videre sies opp med 1 måneds varsel.

4 Partenes ansvarsområde under personopplysningsloven med forskrifter

Sørlandet Sykehus HF er i henhold til Lov om behandling av personopplysninger å anse som databehandlingsansvarlig, jf lovens § 2 nr 4. Den databehandlingsansvarlige har ansvar for å påse at krav, herunder krav til sikkerhet, som stilles i personopplysningsloven med forskrifter er oppfylt. Det innebærer blant annet også at Databehandlingsansvarlig har ansvaret for å påse at kravene er oppfylt i forbindelse med oppbevaring og bruk av personopplysningene hos Databehandleren, jf loven § 15 og forskriften § 2-15.

Databehandleren er å anse som databehandler etter personopplysningsloven § 2 nr 5 og kan kun behandle personopplysninger tilgjengeliggjort av Databehandlingsansvarlig i henhold til denne avtale, jf personopplysningsoven § 15. Eventuell annen bruk av personopplysningene skal i forkant avtales særskilt med Databehandlingsansvarlig.

Databehandleren skal sikre at personopplysninger tilgjengeliggjort av Databehandlingsansvarlig holdes atskilt fra egne og andres opplysninger og tjenester.

Ved avtalens utløp skal Databehandleren påse at alle personopplysninger som er tilgjengeliggjort av Databehandlingsansvarlig makuleres/slettes, slik at opplysningene ikke kan gjenfinnes. I stedet for makulering kan Databehandleren levere tilbake alt utlevert/tilsendt materiale som omfatter personopplysninger tilbake til Databehandlingsansvarlig.

5 Beskrivelse av formålet med bruken av databehandler

Formålet med bruken av databehandler er å regulere tilgangen til persondata, jfr Personopplysningsloven og Helseregisterloven. I dette tilfelle inneholder gjeldende utstyr/system ikke pasientdata, og er heller ikke koplet til nettverk med slike opplysninger.

6 Spesifisering av aktuelle data

Databehandler skal kun logge og overføre data nødvendig for å kunne foreta teknisk logging og vedlikehold på utstyret, og data skal slettes når vedlikeholdet er utført, og dataene ikke er relevante lenger.

Gjeldende utstyr/system ikke har ikke pasientdata, og er heller ikke koplet til nettverk med slike opplysninger.

7 Kontaktpersoner

Følgende kontaktpersoner er oppnevnt i forbindelse med denne avtalen:

- hos Databehandlingsansvarlig: Avdelingsleder Medisinskteknisk Avdeling /SSHF
- hos Databehandleren: Xxxxxxxxxx Xxxxxxx, xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

8 Krav til informasjonssikkerhet

Begge parter skal til enhver tid tilfredsstille krav til informasjonssikkerhet i personopplysningsloven § 13 og personopplysningsforskriften kapittel 2. For helseopplysninger må krav til tilgang sikres iht behov gitt i helselovgivningen.

Databehandleren skal sikre at all behandling av personopplysninger som er omfattet av denne avtalen utføres i samsvar med akseptabelt risikonivå definert av Databehandlingsansvarlig. Gjennomført risikovurdering skal fremlegges av databehandler for egen og eventuelle underleverandørers sikkerhet som del av dette.

Det forutsettes at databehandler har definert sikkerhetsmål, -strategi, -organisering og ansvar i samsvar med Personopplysningsloven og –forskriften og at dette følges opp med nødvendig Internkontrollsystem.

Kompromittering eller mistanke om kompromittering av opplysningene, skal umiddelbart rapporteres til sykehusets personvernombud.

Databehandleren skal ha klare rutiner for logging av feil og avvik som er av betydning for Databehandlingsansvarliges informasjonssikkerhet og som er omfattet av denne avtalen. Dersom det avdekkes slike feil eller avvik, skal Databehandleren så snart som mulig, og senest innen 24 timer, varsle Databehandlingsansvarlig om dette. Databehandleren skal i et slikt tilfelle straks igangsette tiltak for å minimere mulig skade for Databehandlingsansvarlig.

Databehandlingsansvarlig kan til enhver tid kreve dokumentasjon hos Databehandleren for å forsikre seg om at Databehandleren overholder alle relevante krav i personopplysningsloven og –forskriften vedrørende informasjonssikkerhet. Databehandlingsansvarlig kan kreve tilgang til Databehandlerens rapporter mv knyttet til periodiske revisjoner av sine prosedyrer og rutiner.

8.1 Krav til teknisk sikkerhet

Følgende krav til teknisk sikkerhet forutsettes:

- Tilgang til tjenester og opplysninger i nettverket skal være basert på individuelle brukerkoder og passord.

- Lagring av opplysninger overlevert av databehandlingsansvarlig skal sikres, slik at kun autoriserte medarbeidere har tilgang.
- Tilgang til eksterne nett/Internett og Databehandlerens åpne nettverk, dersom det finnes, skal kun være tilgjengelig via tynnklient eller tilsvarende, slik at det ikke er mulig å flytte de utleverte opplysninger fra sikret område til eksterne nett eller interne nett med lavere sikkerhets-funksjonalitet, ref Datatilsynets referansemodell for behandling av sensitive personopplysninger.
- Sikkerhet skal ivaretas ved fjerndrift. Dette innebærer benyttelse av bærbar PC tilhørende Leverandøren, kryptert VPN forbindelse og sperring mot samtidig tilgang til Internett. DriftsPC skal ikke brukes av venner, familie eller andre ikke autoriserte personer.
- 2-nivå autentisering skal benyttes om tilgang skjer via usikre nettverk
- Kommunikasjon skal sikres med kryptering dersom den går over usikre nettverk og det sendes sensitive personopplysninger.

8.2 Krav til tilgangskontroll

Databehandleren har ansvar for at personell (hos Databehandleren eller underleverandører som denne benytter) med elektronisk tilgang til Systemet, alltid skal ha underskrevet taushetserklæring før tilgang gis. Taushetsplikten gjelder også etter at oppdraget er avsluttet og inntil Databehandlingsansvarlig eventuelt skriftlig opphever taushetsplikten for vedkommende.

Databehandleren skal ha rutiner for tilgangsautorisasjon og -styring som sikrer at bare de av Databehandlerens medarbeidere som har reelt behov til tilgang til Systemet og informasjonen for å gjennomføre leveransen/tjenesten, har tilgang. Tilgangsnivå skal være i henhold til reelt behov knyttet til å gjennomføre leveransen.

Databehandler skal til enhver tid ha oversikt over eget personell som er autorisert for tilgang til Databehandlingsansvarliges informasjon og tjenester. På forespørsel skal slik oversikt forelegges Databehandlingsansvarlig.

Dersom Databehandlingsansvarlig har innvendinger mot at en gitt person har fysisk og/eller elektronisk adgang til Systemet, skal autorisasjon for dette inndras.

Det skal benyttes personlige brukerkonti for all tilgang knyttet til gjennomføring av leveransen.

Dersom Databehandleren benytter bærbare klient maskiner til drift, skal Databehandleren ha rutiner som sikrer at disse bare benyttes av driftspersonell og til driftsrelaterte oppgaver.

Dersom tredjepart eller underleverandør i forbindelse med support eller tilsvarende skal ha tilgang til systemet, skal det benyttes midlertidige passord eller tilsvarende. Dette skal endres/sperres umiddelbart når behovet for tilgang opphører.

8.3 Krav til fysisk sikkerhet

Det skal benyttes adgangskontroll med bruk av adgangskort med personlig kode eller tilsvarende. Adgangskontroll til begrensede områder (feks drift og serverrom) skal være basert på faktiske behov. Personell som ikke er autoriserte, skal følges. Adgangskontroll med låste dører gjelder for følgende typer lokaler: datahall/serverrom, IT lokaler (drift/support), lokaler med IT relatert utstyr (koblingsmatriser, svitsjer/rutere), osv.

8.4 Krav om rett til innsyn, inspeksjon og testing

Databehandlingsansvarlig skal ha rett til innsyn i og verifikasjon av hvordan løsningen er sikret. Med innsyn menes dokumentasjon, intervjuer, møte, tester, sikkerhetsovervåking av nettverkstrafikk og aktivitet på server samt eventuelle andre former for verifikasjon som kan være hensiktmessig. Databehandleren aksepterer at innsyn kan gjennomføres av Databehandlingsansvarlig eller den Tredjepart Databehandlingsansvarlig måtte velge til gjennomføring. Retten til innsyn gjelder alle tekniske, organisatoriske og administrative forhold som er relevante for sikkerheten i tjenesten som leveres Databehandlingsansvarlig.

Databehandleren forplikter seg på to ukes varsel å utlevere eller på annen måte sørge for mulighet for innsyn i sikkerhetsmessig dokumentasjon relevant for Databehandlingsansvarlig.

Dersom Databehandlingsansvarlig gjør bruk av retten til innsyn og avvik i sikring av Systemet oppdages, skal Databehandleren uten ugrunnet opphold korrigere avvik. Databehandleren skal skriftlig redegjøre for korrektive tiltak og plan for gjennomføring. Databehandleren skal som en del av kontrakten vederlagsfritt bidra med relevant personell og nødvendig omfang av innsats ved oppfølgning og rettelser av avvik relatert til sikkerhet i Systemet. Dette gjelder når avvik og eventuelle behov for rettelser skyldes handlinger eller mangel på slike hos Databehandleren eller underleverandører denne måtte benytte.

9 Taushetsplikt

Partene skal bevare taushet om alle konfidensielle opplysninger, noens personlige forhold, sikkerhetsmessige og forretningsmessige forhold, opplysninger som kan skade en av partene eller som kan utnyttes av utenforstående i næringsvirksomhet.

Taushetsplikten gjelder partenes ansatte og andre som handler på partenes vegne i forbindelse med gjennomføringen av kontrakten. Alle ansatte skal ha undertegnet taushetserklæring (Taushets-erklæringene skal gi tilsvarende dekning som Databehandlingsansvarliges egne taushetserklæringer.). Kopi av taushetserklæring skal fremlegges på forespørsel og eventuelt korrigeres ved behov.

Partene plikter å ta de forholdsregler som er nødvendig for å sikre at materiale eller opplysninger ikke blir gjort kjent for andre i strid med dette punktet.

Punktet gjelder også etter at kontrakten er opphørt. Ansatte og andre som fratrer sin tjeneste hos en av Databehandlerne skal pålegges taushet også etter fratredelse om forhold som nevnt over.

10 Mislighold

Mislighold foreligger dersom en av partene ikke oppfyller sine plikter etter denne avtalen og dette ikke skyldes forhold som den andre parten har ansvaret for eller risikoen for.

Dersom en av partene ønsker å påberope seg mislighold, skal dette meddeles den andre parten skriftlig uten ugrunnet opphold.

11 Sanksjoner ved mislighold

Ved mislighold kan den krenkede part holde tilbake sin motytelse, men ikke åpenbart mer enn det som synes påkrevd for å avhjelpe virkningene av misligholdet, og bare inntil forholdet er brakt i overensstemmelse med avtalen.

Hvis det foreligger vesentlig mislighold, kan den andre parten – etter å ha gitt skriftlig varsel og rimelig frist til å bringe forholdet i orden – heve hele eller deler av avtalen med øyeblikkelig virkning og kreve erstatning for eventuelle tap dette har medført.

12 Ansvar for underleverandører

Dersom en av partene engasjerer utenforstående (underleverandører) til å utføre ytelser som følger av denne avtalen, er parten fullt ansvarlig for utførelsen av disse ytelsene på samme måte som om han selv stod for utførelsen. Databehandleren skal sørge for at underleverandører undertegner og forplikter seg til å følge Databehandlingsansvarliges databehandleravtale.

13 Overdragelse av rettigheter og plikter

Databehandlingsansvarlig kan helt eller delvis overdra sine rettigheter og plikter etter avtalen til en annen norsk statlig virksomhet, som da er berettiget til tilsvarende vilkår. Databehandleren kan kreve å få dekket eventuelle merutgifter som er forbundet med overdragelsen.

Databehandleren kan overdra sine rettigheter og plikter etter avtalen med skriftlig samtykke fra Databehandlingsansvarlig. Slikt samtykke kan ikke nektes uten saklig grunn. Rett til vederlag etter avtalen kan fritt overdras, men overføring fritar ikke Databehandleren for hans plikter og ansvar.

14 Rettsvalg og verneting

Partenes rettigheter og plikter etter denne avtalen bestemmes i sin helhet av norsk rett.

Eventuelle tvister som springer ut av denne avtalen skal behandles ved de ordinære domstoler. Vest-Agder tingrett vedtas som verneting.

15 Undertegning

Denne avtale er undertegnet i 2- to- eksemplarer, hvorav hver part beholder 1- ett- eksemplar.

Se systemoversikt over gjeldende og aktuelle systemer ved SSHF, vist i vedlegg.

Kristiansand, den .....

……	……
Databehandlingsansvarlig (signatur)	Databehandleren (signatur)
(med trykte bokstaver)	(med trykte bokstaver)
Stilling:……..	Stilling:……..
Navn: …….	Navn: …….

Dato: xx.xx.2013.

Vedlegg.

Avtalen gjelder for xxxxxxxxxxxxxxx anskaffet og montert på Sørlandet Sykehus HF i Xxxxxxxxx 2013.