ST. OLAVS HOSPITAL
UNIVERSITETSSYKEHUSET I TRONDHEIM

DATABEHANDLERAVTALE

I henhold til personopplysningsloven og

EUs Personvernforordning 2016/679

mellom

St. Olavs hospital HF

Org.nr.: 883 974 832

Dataansvarlig

og

Norsk Helsenett SF

Org.nr.: 994 598 759

Databehandler

Datert: februar 2019

1. Om avtalen

Norsk ØNH - Tonsilleregister er et samtykkebasert, nasjonalt, medisinsk kvalitetsregister. St. Olavs hospital HF er dataansvarlig og registeret driftes ved Seksjon for medisinske kvalitetsregistre, St. Olavs hospital. Registerets rapporteringsfunksjon er MRS og databehandler er Norsk Helsenett (NHN). Denne databehandleravtalen (heretter omtalt som "Avtalen") regulerer rettigheter og plikter mellom Dataansvarlig og Databehandler (heretter omtalt som "partene") etter:

Lov av 15. juni 2018 nr. 38 om behandling av personopplysninger (personopplysningsloven);

EU forordning 2016/679/EC av 27.april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (General Data Protection Regulation) (heretter omtalt som "personvernforordningen");

Lov om helseregistre og behandling av helseregistre av 18.mai 2001 nr.24 (helseregisterloven);

Lov om behandling av helseopplysninger ved ytelse av helsehjelp av 20.juni 2014 nr. 42 (pasientjournalloven); og

Enhver lov, forskrift eller annet regelverk som erstatter disse.

Ved motstrid mellom Avtalens regulering og de rammer som følger av personopplysningslovgivningen eller relevant helselovgivning, viker Avtalens regulering.

2. Definisjoner

Begrepene "personopplysninger", "behandling", "dataansvarlig", "databehandler", "brudd på opplysningssikkerhet" og "helseopplysninger" skal forstås slik de er definert i personvernforordningen § 4, helseregisterloven § 2 og pasientjournalloven § 2 som gjeldende.

"Avvik": brudd på opplysningssikkerhet og bruk av informasjonssystemet i strid med fastlagte rutiner.

Bruk av informasjonssystemet som ikke er i samsvar med instrukser fra Behandlingsansvarlig eller gjeldende personvernlovgivning skal behandles som avvik.

3. Avtalens bakgrunn og formål

Denne Avtalen er inngått mellom partene og skisserer de generelle vilkårene for den behandling av helse- og personopplysninger som Databehandler utfører på vegne av Dataansvarlig.

Formålet med Avtalen er å sikre behandlingen av helse- og personopplysninger på vegne av Dataansvarlig slik at helse- og personopplysningene ikke brukes urettmessig eller kommer uberettigede i hende.

4. Omfang

Denne Avtalen kommer til anvendelse på all behandling av helse- og personopplysninger som Databehandler foretar i forbindelse med data registrert i Norsk ØNH - Tonsilleregister (heretter omtalt som "Tjeneste/oppdragsavtalen"). I tilfelle konflikt mellom denne Avtalen og Tjeneste/oppdragsavtalen, skal denne Avtalen gjelde.

Tjenester som inngår i denne Avtalen er de tjenester som inngår i Tjeneste/oppdragsavtalen og som innebærer behandling av helse- og personopplysninger.

Denne Avtalen vil i tillegg gjelde for ytterligere behandling av helse- og personopplysninger basert på eventuelle skriftlige avtaler mellom partene som inngås i løpet av denne Avtalens virksomhetsperiode og som innebærer at Databehandler behandler helse- og personopplysninger på vegne av Dataansvarlig (heretter omtalt som "senere skriftlige avtaler mellom partene").

Personopplysninger skal kun benyttes til de formålene som følger av denne Avtalen, Tjeneste/oppdragsavtalen og senere skriftlige avtaler mellom partene i den utstrekning det er strengt nødvendig for å gjennomføre og imøtekomme kravene i avtalene.

5. Behandlingens formål, opplysninger og behandlinger

Formålet med og varigheten av behandling av helse- og personopplysninger, hvilke helse- og personopplysninger som behandles, kategorier av de registrerte og behandlingens art er angitt i **Vedlegg 1.**

6. Rammene for behandling av helse- og personopplysninger

Dataansvarlig har til enhver tid full rådighet over de helse- og personopplysningene som Databehandler har anledning til å behandle etter denne Avtalen. Databehandler har ikke selvstendig råderett over helse- og personopplysningene, og kan ikke behandle disse til egne formål.

Dataansvarlig har, med mindre annet er avtalt eller følger av lov, rett til tilgang til og innsyn i helse- og personopplysningene som behandles hos Databehandleren.

7. Dataansvarliges plikter

Dataansvarlig skal etterleve de forpliktelser som fremkommer av personopplysningsloven, personvernforordningen, relevant helselovgivning og annen særlovgivning, samt denne Avtalen.

8. Databehandlers plikter

8.1 Generelt

Databehandler forplikter seg til å behandle helse- og personopplysninger kun i samsvar med all relevant lov og regelverk, denne Avtalen, Tjeneste/oppdragsavtalen, Dataansvarliges dokumenterte instruksjoner og andre gjeldende avtaler mellom partene, samt "Norm for informasjonssikkerhet i helse- og omsorgstjenesten". Databehandler skal ikke ved noen handling eller unnlatelse, sette Dataansvarlig i en slik situasjon at Dataansvarlig bryter noen bestemmelse i gjeldende lov og regelverk.

Databehandler skal ikke:

a. behandle helse- og personopplysninger for andre formål eller i større grad enn det som følger av denne Avtalen, Tjeneste/oppdragsavtale og eventuelle senere skriftlige avtaler mellom partene;
b. behandle helse- og personopplysninger utover det som er nødvendig for å oppfylle Databehandlers forpliktelser i henhold til de til enhver tid gjeldende avtaler;
c. utlevere, overlate eller overføre helse- og personopplysninger i noen form på eget initiativ med mindre det er avtalt på forhånd med Dataansvarlig eller Dataansvarlig har godkjent dette skriftlig;
d. samle inn fra eller overføre helse- og personopplysninger til en tredjepart;
e. behandle helse- og personopplysninger de får tilgang eller adgang til gjennom oppdraget fra Dataansvarlig på annen måte enn hva som er angitt i denne Avtalen, Tjeneste/oppdragsavtale og eventuelle senere skriftlige avtaler mellom partene.

Databehandler skal:

a. ha løpende kontroll på alle kategorier av behandlingsaktiviteter utført på vegne av Dataansvarlig;
b. gi Dataansvarlig tilgang til og innsyn i helse- og personopplysninger som behandles hos Databehandleren;
c. føre og vedlikehold en oversikt over alle opplysninger og behandlinger eller dersom det er relevant, protokoll over sine egne behandlingsaktiviteter i henhold til personvernforordningen artikkel 30;
d. treffe alle rimelige tiltak for å sikre at helse- og personopplysningene til enhver tid er korrekte og oppdaterte;
e. etablere rutiner for å slette informasjon når den ikke lenger er nødvendig ut fra formålet med behandlingen og slette informasjon i henhold til fastsatte rutiner og retningslinjer;
f. ha rutiner for og teknisk mulighet til å begrense behandlingen av den registrertes helse- og personopplysninger dersom den registrerte ønsker det med hjemmel i gjeldende lovgivning;

g. påse at samtlige personer som gis tilgang til personopplysninger som behandles på vegne av Dataansvarlig er kjent med denne Avtalen og gjeldende avtaler mellom partene, og er underlagt disse avtalenes bestemmelser;

h sikre at krav til innebygd personvern og personvern som standardinnstilling innfris i Databehandlers løsninger. Dette inkluderer å bygge inn funksjonalitet for å oppfylle personvernprinsipper samt funksjonalitet for å sikre den registrertes rettigheter;

i gi Dataansvarlig nødvendig bistand slik at Dataansvarlig skal kunne oppfylle sine forpliktelser overfor de registrerte;

j samarbeide med og bistå Dataansvarlig ved oppfyllelse av de registrertes rettigheter knyttet til tilgang til opplysninger, herunder å svare på anmodninger fra den registrerte med henblikk på å utøve sine rettigheter fastsatt i personvernforordningen kapittel III;

k omgående underrette den Dataansvarlige dersom Databehandler mener at en instruks er i strid med personvernforordningen eller andre bestemmelser om vern av personopplysninger;

l bistå Dataansvarlig for å sikre overholdelse av forpliktelsene i personvernforordningen artiklene 35-36 som omhandler vurdering av personvernkonsekvenser og forhåndsdrøftinger med Datatilsynet.

8.2. Tekniske, organisatoriske og sikkerhetsmessige tiltak

Databehandler plikter å treffe og gjennomføre alle nødvendige og adekvate planlagte og systematiske tekniske, organisatoriske og sikkerhetsmessige tiltak slik at det til enhver tid er tilfredsstillende informasjonssikkerhet ved behandling av helse- og personopplysninger.

Databehandleren skal:

a. etablere en sikkerhetsorganisasjon med klar ansvarsfordeling, etablere og etterkomme nødvendige tekniske og organisatoriske tiltak med hensyn til vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet ved behandling av helse- og personopplysninger for å sikre tilfredsstillende informasjonssikkerhet i henhold til personopplysningslovgivningens bestemmelser, herunder kravene etter personvernforordningen artikkel 32, og gjeldende helselovgivning. Dette omfatter blant annet, alt etter hva som er relevant, nødvendige tiltak for å forhindre tilfeldig eller ulovlig ødeleggelse eller tap av data, ikke-autorisert tilgang til eller spredning av data så vel som enhver annen bruk av helse- og personopplysninger som ikke er i overensstemmelse med denne Avtalen, og tiltak for å gjenopprette tilgjengelighet og tilgang til opplysningene ved hendelser;
b. ha gode og hensiktsmessige internkontrollrutiner;
c. ha rutiner for autorisasjon og styring som sikrer at bare de av Databehandlers medarbeidere som har reelt behov for tilgang til systemer og opplysningene for å ivareta nødvendige oppgaver for gjennomføring av Tjeneste/oppdragsavtalen får slik tilgang. Tilgangsnivået skal være i henhold til reelt behov knyttet til å gjennomføre oppdraget;
d. etablere nødvendige systemer og rutiner for å ivareta informasjonssikkerheten og følge opp avvik, som skal omfatte blant annet rutiner for avviksmelding, gjenoppretting av normalsituasjonen, fjerne årsaken til avviket og hindre gjentakelse.

På forespørsel, skal Databehandler gi Dataansvarlig tilgang til relevant sikkerhetsdokumentasjon og systemene som benyttes for behandling av helse- og personopplysninger;

e. gjennomføre tiltak for å hindre tilfeldig eller ulovlig ødeleggelse eller tap av personopplysninger, uautorisert innsyn i eller utlevering av personopplysninger samt enhver annen bruk av personopplysninger som ikke er i samsvar med de instrukser som er gitt av Dataansvarlig.
f. hindre uautorisert tilgang til fysiske lokasjoner, systemer, applikasjoner, programvare og utstyr som brukes til behandling av personopplysninger på vegne av Dataansvarlig;
g. hindre at Databehandlers medarbeidere eller systemer bevisst eller ubevisst medvirker til uønskede sikkerhetshendelser i Databehandlers egen virksomhet eller hos andre virksomheter eller privatpersoner;
h. sørge for tilfredsstillende virusbeskyttelse ved hjelp av spam-filtre, IT-policyer, brannmurer mv.
i. rutiner for jevnlige oppdateringer, tilfredsstillende backup-prosedyrer og tester for kritiske systemer
j. etablere rutiner for å slette opplysninger når det ikke lenger er behov for disse i tilknytning til behandlingen av Personopplysninger i henhold til Avtalen.
k. ha rutiner for og teknisk mulighet til å begrense behandlingen av den registrertes helse- og personopplysninger dersom den registrerte ønsker det med hjemmel i gjeldende lovgivning.
l. Kontinuerlig bidra til utvikling av sikkerhetsmessig tilfredsstillende lagringsløsninger for lagring av personopplysninger.
m. **Avvik:** Enhver bruk av informasjonssystemet som er i strid med Databehandlers fastlagte rutiner, den Dataansvarliges instrukser eller Personopplysningslovgivningen, samt ethvert sikkerhetsbrudd, skal behandles som et avvik.
   Databehandler skal ha rutiner og systematiske tiltak for oppfølging av avvik, herunder tiltak for gjenoppretting av normal tilstand, fjerning av årsaken til avviket og hindre gjentakelse.
   Databehandler skal uten unødig opphold rapportere avvik til den Dataansvarlige. Rapporten skal omfatte informasjon om hvilke tiltak Databehandler har gjort for å gjenopprette normal tilstand, fjerne årsaken til avviket og hindre gjentakelse. Databehandler skal også gi Dataansvarlig alle nødvendige opplysninger for å kunne besvare spørsmål fra tilsynsmyndigheter og etterleve krav om varsling til Datatilsynet og berørte registrerte. Databehandler skal påse at medarbeidere som behandler Personopplysninger på vegne av den Dataansvarlige er kjent med denne Databehandleravtalen og sørge for at de er underlagt vilkårene i denne.
n. avdekke, registrere, rapportere og lukke avvik knyttet til informasjonssikkerhet, herunder loggføre og dokumentere ethvert forsøk på ikke-autorisert tilgang og andre brudd på opplysningssikkerheten i datasystemene. Slik dokumentasjon skal oppbevares hos Databehandler;
o. ved mistanke om eller konstatering av avvik, omgående varsle Dataansvarlig. I varselet opplyses avviket med forklaring om årsak, tidsrom og tidspunktet avviket ble oppdaget, kategoriene av og omtrentlig antall registrerte som er berørt, kategoriene av og omtrentlig antall registreringer av personopplysninger som er berørt, navnet på og kontaktopplysningene til personvernombudet eller et annet kontaktpunkt der mer

informasjon kan innhentes, antatte konsekvenser av avviket og hvilke umiddelbare tiltak som er igangsatt eller vurderes igangsatt for å håndtere avviket;

p. dokumentere ethvert avvik, herunder de faktiske forhold knyttet til avviket, dets virkninger og eventuelle iverksatte utbedringstiltak;
q. omgående varsle Dataansvarlig ved uautorisert utlevering av personopplysninger;
r. registrere all autorisert og uautorisert tilgang til informasjon. Alle oppslag som gjøres skal registreres slik at de kan spores til den enkelte bruker (dvs. ansatte hos Databehandler, underleverandører og Dataansvarlig). Loggene skal oppbevares til det ikke lenger antas å være bruk for dem eller i henhold til det Tjeneste/oppdragsavtalen spesifiserer;
s. bistå Dataansvarlig med å sikre overholdelse av forpliktelsene i personvernforordningen artiklene 32–34, dvs:
   - sikkerhet ved behandlingen;
   - melding til tilsynsmyndigheten om brudd på personopplysningssikkerheten;
   - underretning av den registrerte om brudd på personopplysningssikkerheten;
t. i forbindelse med sikkerhetsrevisjon som utføres av Dataansvarlig eller en tredjepart utpekt av Dataansvarlig, framlegge interne revisjonsrapporter, interne prosedyrer, rutiner, sikkerhetsarkitektur, risiko og sårbarhetsanalyser med tiltak og andre dokumenter av betydning for revisjonen;
u. varsle Dataansvarlig om alle forhold som medfører endring i risikobildet;
v. innhente godkjenning av Dataansvarlig før gjennomføring av enhver endring av databehandlingen hos Databehandler som har eller kan ha betydning for informasjonssikkerheten.

Nærmere krav til Databehandlerens informasjonssikkerhet er angitt i **Vedlegg 2.**

Ved brudd på denne Avtalen eller på bestemmelsene i personopplysningslovgivningen, helselovgivningen eller annen relevant lovgivning kan Dataansvarlig kreve endringer i behandlingsmåten eller pålegge Databehandler å stoppe den videre behandlingen av opplysningene med øyeblikkelig virkning.

Databehandler skal dokumentere sine rutiner og alle tiltak truffet for å oppfylle kravene angitt ovenfor. Denne dokumentasjonen skal på forespørsel gjøres tilgjengelig for Dataansvarlig.

9. Sikkerhetsrevisjon

Databehandler er innforstått med at den Dataansvarlige regelmessig kan gjennomføre sikkerhetsrevisjoner av informasjonssystemet og tilhørende fasiliteter som benyttes av Databehandler eller godkjente underleverandører for behandling av Personopplysninger på vegne den Dataansvarlige. Dataansvarlig kan alternativt kreve at sikkerhetsrevisjonen foretas av en uavhengig tredjepart etter anerkjente standarder.

Sikkerhetsrevisjonen skal være rimelig og skal ta hensyn til omfanget av databehandlingen og skal blant annet omfatte en vurdering av Databehandlers organisering, relevante sikkerhetstiltak og Databehandlers bruk av underleverandører.

Dersom sikkerhetsrevisjonen avdekker uforutsett bruk av informasjonssystemet skal dette behandles som avvik.

Resultatet fra sikkerhetsrevisjon skal dokumenteres og rapporten fra sikkerhetsrevisjonen skal utleveres til den Dataansvarlige.

10. Bruk av underleverandør

Dataansvarlig tillater at Databehandler benytter underleverandører for oppfyllelse av forpliktelsene under Avtalen. Databehandler benytter underleverandører som angitt i **Vedlegg 3** for de der angitte tjenester og bekrefter at det er ingen andre underleverandører som benyttes.

Databehandler skal:

a. sikre at underleverandøren påtar seg tilsvarende forpliktelser som Databehandler under Avtalen og gjeldende lovgivning;
b. sørge for at underleverandører kun behandler personopplysninger i samsvar med denne Avtalen og ikke i større utstrekning enn det som er nødvendig for å oppfylle den aktuelle tjenesten som underleverandøren leverer;
c. holde en oppdatert liste over identiteten og stedlig plassering av underleverandører som angitt i **Vedlegg 3**. Oppdatert liste skal være tilgjengelig for Dataansvarlig;
d. gjennomføre en risikovurdering av bruk av underleverandør og betydningen for tjenesten før det inngås avtale med underleverandør og på Dataansvarliges forespørsel, dele vurderingen med Dataansvarlig;
e. på Dataansvarliges forespørsel, legge frem kopi av avtalen(e) som er inngått med underleverandørene (med unntak av merkantile betingelser). Slike avtaler skal senest være inngått før underleverandørene starter med behandling av helse- og personopplysninger;
f. underrette Dataansvarlig om eventuelle planer om å benytte andre underleverandører eller skifte ut underleverandører. Slike bytter skal varsles i god tid slik at Dataansvarlig gis mulighet til å motsette seg endringen. Ved bytte av underleverandør skal **Vedlegg 3** oppdateres og oversendes Dataansvarliges kontaktperson. Hvis dataansvarlig ikke aksepterer skifte av underleverandør og databehandler ikke kan finne en annen underleverandør som dataansvarlig kan akseptere, kan Dataansvarlig si opp avtalen med umiddelbar virkning. Se pkt. 14. Varighet og opphør.
g. sikre at Dataansvarlig og tilsynsmyndighetene har samme rett til innsyn og kontroll med behandling av personopplysninger hos en underleverandør som Dataansvarlig har overfor Databehandler etter Avtalens punkt 12;
h. ved opphør av Avtalen, sikre at underleverandører oppfyller plikten til å slette eller forsvarlig destruere alle helse- og personopplysningene og alle eventuelle kopier og sikkerhetskopier av opplysningene som framgår av Avtalens punkt 13 på samme måte som Databehandler så langt det ikke strider mot andre lovbestemmelser.

Databehandler er til enhver tid fullt ut ansvarlig overfor Dataansvarlig for alt arbeid som utføres av underleverandører og for underleverandørenes etterlevelse av bestemmelsene i denne Avtalen.

Tilgang til helse- og personopplysninger for tredjeparter krever konkret avtale utover denne Avtalen mellom partene for alle andre enn Databehandlers underleverandører.

11. Overføring av personopplysninger til utlandet

Partene i denne Avtalen er enige om at ingen av helse- og personopplysningene som behandles under denne Avtalen skal føres ut av Norge, med mindre det er særskilt avtalt mellom partene. I tillegg skal helse- og personopplysninger være plassert på servere i Norge (jf. arkivloven § 9 bokstav b). Eventuelle unntak som innebærer overføring til utlandet skal godkjennes eksplisitt av Dataansvarlig før behandlingen starter.

Databehandler bekrefter at ingen av underleverandørene overfører helse- og personopplysninger som omfattes av denne Avtalen til utlandet, med unntak for slike overføringer som er angitt i **Vedlegg 3**. Dette omfatter også fjerntilgang fra utlandet.

Bruk av underleverandører som overfører helse- og personopplysninger til land utenfor EU/EØS (tredjeland) skal avtales skriftlig med Dataansvarlig på forhånd. Ved overføring av helse- og personopplysninger til land utenfor EU/EØS (tredjeland) skal Databehandler benytte godkjente EU-overføringsmekanismer.

Ved overføring til utlandet, uavhengig av om det er innenfor EU/EØS eller utenfor EU/EØS (tredjeland), skal Databehandler gi nødvendig dokumentasjon om sikkerhet, risiko og etterlevelsesnivå knyttet til aktuelle underleverandører slik at Dataansvarlig får nødvendig informasjon for å kunne gjennomføre en særskilt risikovurdering. Dataansvarlig kan nekte samtykke til den aktuelle overføringen basert på spesifikke risikoer som fremkommer av Dataansvarliges egen risikovurdering.

12. Taushetsplikt

Databehandlers ansatte og andre som opptrer på Databehandlers vegne i forbindelse med behandling av personopplysninger i henhold til denne Avtalen, Tjeneste/oppdragsavtale og senere skriftlige avtaler mellom partene (heretter omtalt som «personer som er autorisert til å behandle personopplysningene»), er underlagt taushetsplikt etter denne Avtalen og gjeldende regelverk. Personer som er autorisert til å behandle personopplysningene forplikter seg til å behandle opplysningene fortrolig. Det samme gjelder eventuelle underleverandører.

Databehandler skal påse at alle som behandler personopplysninger under Avtalen er kjent med taushetsplikten.

Ansatte og andre som opptrer på Databehandlers vegne i forbindelse med behandling av personopplysninger skal ha undertegnet taushetserklæring.

Partene har i tillegg taushetsplikt om konfidensiell informasjon knyttet til hverandres virksomhet, som er formidlet i forbindelse med oppdraget.

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

Taushetsplikten gjelder også etter Avtalens opphør.

13. Innsyn, verifikasjon og revisjon

Dataansvarlig kan til enhver tid kreve innsyn i og verifikasjon av Databehandlers behandling av personopplysninger tilhørende Dataansvarlig, herunder innsyn i og verifikasjon av dokumentasjon for oppfyllelse av kravene til informasjonssikkerhet og Databehandlers system for internkontroll.

Retten til innsyn gjelder alle tekniske, organisatoriske og administrative forhold som er relevante for sikkerheten ved behandlingen som utføres av Databehandler på vegne av Dataansvarlig, og øvrige innsynsrettigheter nedfelt i lov. Hvis Dataansvarlig ber om innsyn skal generell informasjon fra revisjonen gjøres tilgjengelig for andre behandlingsansvarlige som benytter samme tjeneste hos Databehandler.

Dataansvarlig skal så vidt mulig gi Databehandler varsel i rimelig tid ved krav om innsyn og kontroll, vanligvis minst 30 dagers varsel. For krav om dokumentinnsyn bør det gis minst 14 dagers varsel. Dataansvarlig skal medvirke til at innsyn og kontroll kan koordineres mellom flere Dataansvarlige som får levert tjenester fra Databehandler. Innsyn og kontroll kan gjennomføres av Dataansvarlig eller tredjepart som Dataansvarlig utpeker. Databehandler kan kreve dekket dokumenterte merkostnader som påløper ved slike revisjoner.

Databehandler skal gi Datatilsynet og annen relevant tilsynsmyndighet tilgang og innsyn i behandlingen av helse- og personopplysninger slik det følger av relevant lovgivning.

Databehandler skal uten ugrunnet opphold korrigere eventuelle avvik. Avvik som skyldes Databehandler eller dennes underleverandører skal korrigeres uten kostnad for Dataansvarlig. Databehandler skal skriftlig redegjøre for korrektive tiltak og plan for gjennomføring.

14. Varighet og opphør

Denne Avtalen gjelder fra den er signert av partene og gjelder til Avtalen og alle gjeldende avtaler mellom partene, som innebærer at Databehandler skal behandle helse- og personopplysninger på vegne av Dataansvarlig, er opphørt.

Ved opphør av Avtalen skal Databehandler tilrettelegge for og medvirke til tilbakeføring av alle opplysninger som Databehandler har mottatt og behandlet på vegne av Dataansvarlig. Partene avtaler nærmere hvordan overføring konkret skal skje.

Etter at alle opplysningene er overført til Dataansvarlig og bekreftet mottatt av denne, skal Databehandler irreversibelt slette eller forsvarlig destruere alle opplysningene og alle eventuelle kopier og sikkerhetskopier av opplysningene i sine systemer, med mindre ufravikelige rettsregler krever at helse- og personopplysningene fortsatt lagres.

Benyttes delt infrastruktur der direkte sletting ikke er teknisk mulig skal Databehandler sørge for at data gjøres utilgjengelig inntil disse dataene er overskrevet av systemet.

Databehandler skal gi Dataansvarlig skriftlig bekreftelse på at opplysningene er overført og slettet som angitt over.

15. Endring av avtale

I tilfelle endringer i gjeldende lovverk, endelig dom som gir en annen tolkning av gjeldende lov, eller endringer i tjenester i Tjeneste/oppdragsavtalen som krever endringer av denne Avtalen, skal partene samarbeide for å oppdatere Avtalen tilsvarende.

16. Meddelelser

Meddelelser, underretting, varsel eller annen kommunikasjon mellom Dataansvarlig og Databehandler skal gis skriftlig, eller bekreftes skriftlig til:

Dataansvarlig	Databehandler
St. Olavs hospital Seksjon for medisinske kvalitetsregistre, MTFS, v/ Elin Tollefsen Postboks 3250, Torgarden, 7006 Trondheim	**Norsk Helsenett SF** Postboks 6123 7435 Trondheim
Navn: Elin Tollefsen Rolle: overlege dr.med. / rådgiver, Seksjon for medisinske kvalitetsregistre, MTFS. E-post: elin.tollefsen@stolav.no Mobilnr.: 975 70 946	Navn: Ågot Ligaarden Rolle: Tjenesteansvarlig E-post: agot.ligaarden@nhn.no Mobilnr.: 959 77 349

17. Lovvalg og verneting

Avtalen er underlagt norsk rett og partene vedtar Sør-Trøndelag tingrett som verneting. Dette gjelder også etter opphør av Avtalen.

18. Undertegning

Denne Avtalen foreligger i to originaler, hvorav partene beholder et eksemplar hver.

Sted og dato:

Trondheim, februar 2019

Dataansvarlig	Databehandler
St. Olavs hospital HF v/ Direktør	**Norsk Helsenett SF**
Navn:	Navn:

VEDLEGG 1 – BEHANDLINGENS FORMÅL, OPPLYSNINGER OG BEHANDLINGER

Tabellene oppdateres fortløpende.

Februar 2019

A. Formålet med og varigheten av behandlingen

Formålet med og varigheten av behandling av helse- og personopplysninger er:

Navn på tjeneste	Formålet med behandlingen	Varigheten av behandlingen
Norsk ØNH - Tonsilleregister	Formålet er å sikre en hensiktsmessig og trygg behandling for hele pasientgruppen, samt å øke kunnskapen om behandlingen både for den enkelte pasient og for pasientgruppen i sin helhet.	Personopplysninger samles inn i henhold til samtykke med hjemmel i Helseregisterloven §9 og lagres så lenge registeret har et behandlingsgrunnlag.
Drift av MRS, innsamling og tilgjengeliggjøring av data	Eks. innregistrering, lagring, rapporter, Resultatportalen.	Så lenge det foreligger en hjemmel
Filoverføringstjenesten	Overføre større datamengder.	Så lenge det foreligger en hjemmel. Tjenesten er foreløpig ikke tatt i bruk av Tonsilleregisteret, men registeret søker om tilgang til tjenesten så snart den er på plass.
Innsynstjenesten	Pasienter får innsyn i egne data.	Så lenge det foreligger en hjemmel. Tjenesten er foreløpig ikke tatt i bruk av Tonsilleregisteret, men registeret søker om tilgang til tjenesten så snart den er på plass.
ePROM	Elektronisk utsendelse av skjema til pasientene.	Så lenge det foreligger en hjemmel. Det er et mål at alle nasjonale registre skal ha denne tjenesten.

Pasientrapportering på papir (PIPP)	Løsningen til HEMIT for å sende ut skjema via posten.	Så lenge det foreligger en hjemmel. Det er et mål at alle nasjonale registre skal ha denne tjenesten.
FALK	Tilgangsstyring av brukere.	Så lenge det foreligger en hjemmel.
Rapporteket	Resultatformidling.	Så lenge det foreligger en hjemmel. Tjenesten er foreløpig ikke tatt i bruk av Tonsilleregisteret, men det er et nasjonalt mål at nasjonale medisinske kvalitetsregistre, inkludert Tonsille-registeret, skal ta i bruk Rapporteket.
Helseregisterpålogging	Tilgang.	Så lenge det foreligger en hjemmel.

B. Behandling av helse- og personopplysninger

Databehandlers behandlingsaktiviteter som omfattes av Avtalen:

Behandling	Behandlingsaktiviteter
Innsamling	Innsamling av person- og helseopplysninger om pasienter til medisinske kvalitetsregistre
Tilgjengeliggjøring	Tilgjengeliggjøring av person- og helseopplysninger i medisinske kvalitetsregistre for aktører med tilgang til tjenesten for innsyn, registrering, endring og sletting
Lagring	Lagring av person- og helseopplysninger samlet inn i medisinske kvalitetsregistre. Alle opplysninger blir behandlet i samsvar med gjeldende lover og forskrifter.
Tilpasning eller endring	Tilpassing og endring av data på forespørsel fra Dataansvarlig
Sammenstilling	Sammenstilling av data for rapportering, analyse og statistikk
Sletting eller tilintetgjøring	Sletting av register ved eventuell opphør av tjenesten, eller av pasients egne opplysninger hvis pasient krever det. Sletting av data vil ikke innebære sletting fra

	anonymiserte forskningsfiler som allerede er benyttet i forskning.
Utlevering/Overføring	Utlevering/overføring av opplysninger til helsepersonell eller andre aktører på forespørsel fra Dataansvarlig

C. Typer av opplysninger

Følgende helse- og personopplysninger behandles:

Personopplysninger	Helseopplysninger
Navn	Diagnosekoder
Fødselsnummer	Prosedyrekoder / operasjonskoder
Bosted	Post-operative komplikasjoner

D. Kategorier av registrerte

Følgende kategorier av personer behandles det opplysninger om (registrerte):

Kategorier av registrerte		
Pasienter	Helsepersonell	
Barn		
Foreldre		

VEDLEGG 2 – DETALJERTE KRAV TIL INFORMASJONSSIKKERHET

Februar 2019

Registeret har konsesjon fra Datatilsynet. Etter innføring av GDPR skjer drift i samsvar med Data Protection Impact Assessment (DPIA) for St. Olavs hospital HF.

Nr.	Tema	Krav
1.	Norm for informasjonssikkerhet i helse- og omsorgssektoren	Registeret følger til enhver tid gjeldende norm.
2.	Sikring av data	Opplysninger i registeret lagres i avidentifisert form, det vil si at personnummeret er erstattet med en kode. Alle data lagres med tilgangsstyrt lagring på sikkert område.
3.	Autentisering	Ved tilgang til data ved tjenstlig behov skal det benyttes personlige brukernavn med passord. MRS-Hemit har etablert passordpolicy.
4.	Logging og sporbarhet	Er på plass i registeret via MRS-Hemit
5.	Sletting og tilbakelevering	Pasienten kan når som helst kreve at opplysninger blir slettet fra registeret, uten å oppgi noen grunn. Sletting av data vil ikke innebære sletting fra anonymiserte forskningsfiler som allerede er benyttet i forskning.
6.	Lagringstid	Personopplysninger samles inn i henhold til samtykke med hjemmel i Helseregisterloven § 9 og lagres så lenge registeret har et behandlingsgrunnlag.
7.	Kryptering ved lagring	Opplysninger i registeret lagres i avidentifisert form, det vil si at personnummeret er erstattet med en kode.
8.	Testdata	Dataansvarliges data skal ikke benyttes for testformål uten at det er avtalt skriftlig med Dataansvarlig. Eventuell anonymisering skal skje på instruks fra Dataansvarlig. I tilfeller der Dataansvarliges data benyttes til test etter avtale, skal disse sikres på samme måte som produksjonsdata. Der det benyttes produksjonsdata til testformål, skal disse slettes etter at test er utført.

VEDLEGG 3 – UNDERLEVERANDØRER

(Liste over hvilke underleverandører som benyttes av Databehandler)

Tabellen oppdateres fortløpende.

Februar 2019

Navn på underleverandør	Leveranseområde	Stedlig plassering
Helse Nord IKT	Rapporteket: drift, systemvedlikehold, brukerstøtte	Tromsø, Norge
Helse Nord IKT	Tilgangsløsning Helseregister.no: drift, systemvedlikehold, brukerstøtte	Tromsø, Norge