Databehandleraftale : Databehandleraftale

Indgået mellem databehandler:
Sundhed.dk - Sentinel
Forskerparken 10
5230 Odense M

Dataansvarlig:
Sven Johansen
Lyngbyvej 24,st
2100 København Ø

Aftalen er underskrevet elektronisk den 02-06-2020 af Sven Johansen

(Den Dataansvarlige og Databehandleren er i det følgende hver for sig benævnt "Part" og under et "Parterne")

Parterne har indgået følgende databehandleraftale ("Aftale"):

Bilag:
Bilag A: Instruks med oplysninger om databehandlingen
Bilag B: Formål og supplerende instruks om databehandlerens behandling af Personoplysninger for Dataansvarlig
Bilag C: Sikkerhedsinstrukser

Indhold

1. Baggrund
1.1 Denne aftale, der har til formål at sikre, at Databehandleren overholder de til enhver tid gældende regler om datasikkerhed, er indgået i forbindelse med Databehandlerens levering af Serviceydelser i form af IT programmet Sentinel, der skal anvendes til de formål, der er beskrevet i bilag A og B (herefter omtalt som "Serviceydelser").

1.2 Aftalen regulerer forhold i relation til Serviceydelserne, gældende databeskyttelseslovgivning, jurisdiktion mv. mellem Parterne. I tilfælde af uoverensstemmelse mellem Parterne har Aftalen forrang for alle andre aftaler mellem Parterne, såfremt det omhandler forhold vedrørende behandling af personoplysninger.
1.3 Databehandleren er bekendt med Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger ("Databeskyttelsesforordningen"), som trådte i kraft den 24. maj 2016 og er gældende fra den 25. maj 2018 samt den supplerende, nationale lovgivning, som gælder sideløbende med Databeskyttelsesforordningen, herunder navnlig lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger ("Databeskyttelsesloven").
1.4 Enhver henvisning til persondatalovgivningen mv. er en henvisning til den til enhver tid gældende lovgivning mv.

2. Personoplysninger og databehandling
2.1 "Personoplysninger" omfatter "enhver form for information om en identificeret eller identificerbar fysisk person; ved identificerbar fysisk person forstås en fysisk person, der direkte eller indirekte kan identificeres, navnlig ved en identifikator som f.eks. et navn, et identifikationsnummer, lokaliseringsdata, en online-identifikator eller et eller flere elementer, der er særlige for denne fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sociale identitet" (jf. Databeskyttelsesforordningen artikel 4, nr. 1) og/eller som termen er defineret i den for den Dataansvarlige gældende Databeskyttelseslovgivning.
2.2 Aftalen finder anvendelse i forhold til Personoplysningerne, Registrerede, Formål samt øvrige forhold og forpligtelser, der vedrører behandlingen af data, og som er defineret og anført i Bilag A, B og C.
2.3 Bilag A, B og C indgår i begge Parters dokumentationsmateriale i henhold til persondatalovgivningen og skal altid afspejle de faktiske forhold.

3. Roller og instrukser
3.1 Databehandleren er databehandler i henhold til gældende lovgivning og behandler Personoplysninger på vegne af den Dataansvarlige, som er dataansvarlig i henhold til gældende lovgivning.
3.2 Den Dataansvarlige træffer beslutning om, til hvilke formål og hvordan Databehandleren må behandle Personoplysningerne. Databehandleren må ikke behandle Personoplysningerne til sine egne formål.
3.3 Databehandleren må i leveringen af Serviceydelser kun behandle Personoplysninger i henhold til dokumenterede instrukser fra den Dataansvarlige, jf. databeskyttelsesforordningens artikel 28, stk. 3, litra a, navnlig for så vidt angår overførsler til tredjelande og en international organisation, medmindre det følger af den EU/EØS-lovgivning eller EU/EØS-medlemsstaternes lovgivning, som Databehandleren er underlagt. I så fald skal Databehandleren underrette den Dataansvarlige i detaljer om sådanne lovkrav, før behandlingen finder sted, medmindre det er forbudt at foretage en sådan underretning af hensyn til vigtige samfundsmæssige interesser.
3.4 Databehandleren må kun ændre, slette og bortskaffe Personoplysninger fra Sentinel efter instruks fra den Dataansvarlige. Databehandleren må dog behandle, herunder bl.a. isolere, flytte og slette, Personoplysninger på anden vis, hvis det er nødvendigt for at imødegå, herunder for at begrænse, et brud på persondatasikkerheden, herunder men ikke begrænset til malware, ransomware, virus og lignende. I tilfælde af sletning skal Dataansvarliges samtykke, om muligt, indhentes. Hvis det vurderes sikkerhedsmæssigt ansvarligt skal der sikres en kopi af materialet inden sletning.

4. Fortrolighed
4.1 De Personoplysninger, som Databehandleren modtager fra den Dataansvarlige, eller som Databehandleren kommer i besiddelse af i forbindelse med leveringen af Serviceydelser, er fortrolige eller personfølsomme og må ikke kopieres, videregives eller behandles uden den Dataansvarliges udtrykkelige og forudgående tilladelse.
4.2 Databehandleren skal sikre, at kun de medarbejdere, for hvem det til enhver tid er nødvendigt at behandle Personoplysninger i forbindelse med udførelsen af deres arbejde, er autoriseret hertil.
4.3 Databehandleren skal sikre, at enhver person, der udfører arbejde for Databehandleren, og som får adgang til Personoplysningerne, kun behandler sådanne oplysninger efter instruks fra den Dataansvarlige, medmindre behandlingen er påkrævet i henhold til EU/EØS-lovgivningen eller EU/EØS-medlemsstaternes nationale lovgivning.
4.4 Databehandleren skal sikre, at de personer, der er autoriserede til at behandle Personoplysninger, har påtaget sig en kontraktuel fortrolighedsforpligtelse eller er underlagt en lovbestemt tavshedspligt.

5. Databehandlerens bistand til den Dataansvarlige
5.1 Under hensyn til behandlingens karakter og de oplysninger, der er tilgængelige for Databehandleren, skal Databehandleren bistå den Dataansvarlige med at sikre overholdelse af forpligtelserne i henhold til artikel 32 til 36 i Databeskyttelsesforordningen, dvs. sikkerhedsforanstaltninger, underretning af tilsynsmyndigheder, underretning af individuelle personer, udarbejdelse af konsekvensanalyser vedrørende databeskyttelse og forudgående høring hos

tilsynsmyndigheder.
5.2 Såfremt der sker brud på persondatasikkerheden og såfremt dette udløser en pligt til at foretage anmeldelse til tilsynsmyndigheden, er det aftalt mellem parterne, at det påhviler Databehandleren at foretage denne anmeldelse på den Dataansvarliges vegne uden unødig forsinkelse og senest 72 timer, efter at Databehandleren er blevet bekendt med det pågældende brud på persondatasikkerheden, dog med forudgående orientering til den Dataansvarlige forinden anmeldelsen afsendes til tilsynsmyndigheden. Jf. afsnit 7.3 vedr. underretning af den Dataansvarlige.
5.3 På tilsvarende vis er det aftalt, at Databehandleren underretter de Registrerede på den Dataansvarliges vegne ved brud på persondatasikkerheden, der sandsynligvis vil indebære en høj risiko for de Registrerede, dog med forudgående orientering til den Dataansvarlige forinden underretningen afsendes til de registrerede.
5.4 Under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for Databehandleren, skal Databehandleren gennemføre passende tekniske og organisatoriske foranstaltninger for at bistå den Dataansvarlige med overholdelsen af den Dataansvarliges lovmæssige forpligtelser under Kapitel III i Databeskyttelsesforordningen, dvs. besvare anmodninger fra Registrerede, der udøver deres lovmæssige rettigheder, herunder, men ikke begrænset til, adgang til, berigtigelse eller sletning af Personoplysninger, begrænsning af behandlingen af Personoplysninger, dataportabilitet og retten til at gøre indsigelse imod automatiske individuelle afgørelser, herunder profilering.

6. Sikkerhed mv.
6.1 Databehandleren skal bistå den Dataansvarlige med at sikre, at den Dataansvarliges lovbestemte forpligtelser overholdes med hensyn til sikkerhed som anført i Aftalen og gældende lovgivning.
6.2 Databehandleren skal implementere passende tekniske og organisatoriske foranstaltninger for at beskytte Personoplysningerne. Sådanne foranstaltninger fastsættes under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder og skal passe til disse risici, som behandlingen udgør, jf. databeskyttelsesforordningens artikel 32, stk. 1, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring eller uautoriseret videregivelse af eller adgang til Personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet. Dette kan inkludere, men er ikke begrænset til, jf. databeskyttelsesforordningens artikel 32, stk. 1, litra a-d:
a) pseudonymisering og kryptering af Personoplysninger,
b) evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester,
c) evne til rettidigt at genoprette tilgængeligheden af og adgangen til Personoplysninger i tilfælde af en fysisk eller teknisk hændelse, eller
d) en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.
6.3 Databehandleren skal nærmere gennemføre de sikkerhedsforanstaltninger, der er anført i Bilag C.
6.4 Den Dataansvarlige har ansvaret for at indrette de processer, der udføres i systemet, der leveres som Serviceydelser således, at de overholder Databeskyttelseslovgivningens krav til databeskyttelse gennem design og databeskyttelse gennem standardindstillinger, jf. kravet i Databeskyttelsesforordningens artikel 25.

7. Sikkerhedsbrud
7.1 Definition
7.1.1 Ved et "Sikkerhedsbrud" forstås, jf. databeskyttelsesforordningens artikel 4, nr. 12, et brud på sikkerheden, som fører til en hændelig eller ulovlig tilintetgørelse, tab, ændring eller uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.
7.2 Log over sikkerhedsbrud
7.2.1 Databehandleren skal til enhver tid føre et register over Databehandlerens sikkerhedsbrud med detaljer om bruddene i forbindelse med Databehandlerens databehandling af Personoplysningerne. Databehandleren skal efter anmodning give den Dataansvarlige en kopi deraf.
7.3 Underretning af den Dataansvarlige
Databehandleren skal uden unødig forsinkelse underrette den Dataansvarlige ved mistanke om eller konstatering af et sikkerhedsbrud med betydning for Personoplysningerne.
7.3.1 Under hensyn til karakteren af behandlingen samt oplysningerne, der er tilgængelige for Databehandleren, er det aftalt, at Databehandleren efter et sikkerhedsbrud straks skal bistå den Dataansvarlige med at sikre overholdelse af den Dataansvarliges lovmæssige forpligtelser i forbindelse med underretning om sikkerhedsbrud til tilsynsmyndigheder og de Registrerede, derved at Databehandleren forestår anmeldelsen til tilsynsmyndigheder og underretninger til de Registrerede på den Dataansvarliges vegne i overensstemmelse med Aftalens punkt 5.
Derudover skal Databehandleren efter et sikkerhedsbrud under hensyn til karakteren af behandlingen, og i det omfang oplysningerne er tilgængelige for Databehandleren, uden unødig forsinkelse give den Dataansvarlige passende og tilstrækkelige oplysninger om det skete sikkerhedsbrud. Databehandleren skal levere følgende oplysninger skriftligt til den

Dataansvarlige:
Karakteren af bruddet:
a) En beskrivelse af de berørte systemer og processer
b) Hvem og hvor mange er berørt
c) En beskrivelse af årsagen til Sikkerhedsbruddet
d) Tidspunktet for indtrædelsen af Sikkerhedsbruddet
e) Varighed af sikkerhedsbruddet
f) Information om, hvorvidt sikkerhedsbruddet fortsat består, eller om det er bragt til ende, og, i så fald, hvordan, og hvis ikke, hvornår det forventes at blive bragt til ende
Sandsynlige konsekvenser:
g) En begrundet vurdering af, om Sikkerhedsbruddet sandsynligvis vil medføre en risiko for fysiske personers rettigheder og frihedsrettigheder
Foranstaltninger for at begrænse skaden:
h) En oversigt over de tiltag, som Databehandleren allerede har iværksat, og i hvor høj grad tiltagene har begrænset eller afhjulpet Sikkerhedsbruddet
i) En oversigt over de tiltag, som Databehandleren planlægger at iværksætte for at følge op på Sikkerhedsbruddet, den forventede tidsramme, og i hvor høj grad tiltagene vurderes at begrænse og/eller afhjælpe Sikkerhedsbruddet
j) En beskrivelse af hvilke foranstaltninger der kunne have forhindret Sikkerhedsbruddet.
7.3.2 Hvis og i det omfang det ikke er muligt at levere oplysningerne anført i pkt. 7.3.1 samlet, kan oplysningerne leveres gradvist. Den gradvise levering skal foregå uden unødige forsinkelser.
7.3.3 I det omfang en eller flere af de oplysninger, der er nævnt under pkt. 7.3.1 ændres efter, at den Dataansvarlige har modtaget oplysningerne, skal Databehandleren straks give den Dataansvarlige de opdaterede oplysninger med markering af, hvor de afviger fra de tidligere fremsendte oplysninger.
7.3.4 Hvis Sikkerhedsbruddet sker hos en underdatabehandler, skal Databehandleren forestå kontakten til underdatabehandleren, medmindre andet aftales mellem Parterne.

8. Underdatabehandlere
8.1 Databehandleren må gøre brug af en anden databehandler (underdatabehandlere) uden forudgående specifik godkendelse fra den Dataansvarlige, forudsat at Databehandleren skriftligt senest 14 dage forinden det planlagte opstartstidspunkt underretter den Dataansvarlige om identiteten på den potentielle underdatabehandler inden indgåelse af aftale med den pågældende underdatabehandler, hvorved den Dataansvarlige får 14 dage til at gøre indsigelse mod ændringer eller tilføjelser. Den Dataansvarliges indsigelse skal indeholde tungtvejende saglige grunde mod anvendelse af den påtænkte underdatabehandler, for at Databehandleren forpligtiges til at efterkomme indsigelsen.
Den Dataansvarlige har ved denne Aftales indgåelse godkendt at Databehandler anvender de underdatabehandlere, som er anført i bilag A.
Hvis der sker tilføjelse, fjernelse eller udskiftning af underdatabehandlere, fremsender Databehandleren underretning om ændring af listen over underdatabehandlere til den Dataansvarlige.
8.2 Det er en forudsætning for antagelse af en underdatabehandler, at Databehandleren indgår en skriftlig aftale med underdatabehandleren om, at underdatabehandleren pålægges de samme databeskyttelsesforpligtelser, som dem der er fastsat i denne Aftale, herunder at underdatabehandleren skal gennemføre passende tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen opfylder kravene i persondatalovgivningen.
8.3 Databehandleren er ansvarlig over for den Dataansvarlige for eventuelle underdatabehandlere på samme måde som for Databehandlerens egne handlinger og undladelser.

9. Placering af Personoplysninger
9.1 Databehandleren må, jf. databeskyttelsesforordningens artikel 28, stk. 3, litra a, kun overføre personoplysninger til et land uden for EU/EØS eller internationale organisationer i det omfang den Dataansvarlige godkender dette, eller hvis det kræves i henhold til EU-retten eller national ret, som Databehandleren er underlagt. I så fald underretter Databehandleren den Dataansvarlige om dette retlige krav, medmindre den pågældende ret også forbyder en sådan underretning.
9.2 Overførsel af personoplysninger uden for EU/EØS må i alle tilfælde kun ske, hvis Databehandleren har sikret et fornødent overførelsesgrundlag, f.eks. EU Kommissionens Standardkontraktsbestemmelser med de hertil nødvendige tillæg for overholdelse af Databeskyttelsesforordningen.
9.3 Hvis det i henhold til det anvendte overførselsgrundlag kræves, at den Dataansvarlige er direkte part heri, er Databehandleren bemyndiget til at gennemføre dette på den Dataansvarliges vegne, f.eks. ved at indgå aftale ved brug af EU Kommissionens Standardkontraktsbestemmelser, med de hertil nødvendige tillæg for overholdelse af Databeskyttelsesforordningen, på vegne af den Dataansvarlige. Databehandleren skal snarest muligt orientere den Dataansvarlig, hvis denne bemyndigelse udnyttes.

9.4 Regulering gældende i medfør af det anvendte overførelsesgrundlag har forrang frem for reguleringen i denne Aftale, dog alene i relation til den behandling, som nødvendiggør overførelsesgrundlaget; øvrig behandling er alene reguleret af denne Aftale.
9.5 Databehandleren underretter den Dataansvarlige om eventuelle yderligere forpligtelser, som den Dataansvarlige kan blive underlagt som følge af lovgivningen i et land udenfor EU/EØS, som Databehandleren overfører personoplysninger til.

10. Påvisning af overholdelse, revisioner mv.
10.1 Databehandleren skal efter anmodning stille alle de oplysninger til rådighed for den Dataansvarlige, der er nødvendige for at påvise overholdelse af databeskyttelsesforpligtelserne under Aftalen og gældende Databeskyttelseslovgivning.
10.2 Databehandleren skal en gang årligt stille en revisionsrapport, der er udarbejdet af en uafhængig it-kyndig tredjepart, til rådighed for den Dataansvarlige med oplysninger, der påviser, om Databehandleren overholder Aftalen. Rapporten skal udformes under hensyntagen til den fortrolighed, der er knyttet til behandlingen af følsomme oplysninger om helbredsforhold.
10.3 Databehandleren skal derudover give mulighed for og bidrage til revisioner og inspektioner, der foretages af den Dataansvarlige eller revisorer bemyndiget af den Dataansvarlige, de offentlige myndigheder i Danmark eller af anden kompetent jurisdiktion, i det omfang det er relevant for at kontrollere, at Databehandleren overholder Aftalen og gældende persondatalovgivning. Den pågældende revisor skal være underlagt tavsheds- og fortrolighedsforpligtelse, enten aftalemæssigt eller ved lov, hvorpå Databehandleren kan støtte direkte ret. Udføres revision af en anden end den Dataansvarlige selv, skal denne anden revisor være uafhængig og ikke-konkurrerende i forhold til Databehandleren.

11. Ændringer til Aftalen
11.1 Aftalen kan ændres, hvis det godkendes af både den Dataansvarlige og Databehandler. Den Dataansvarlige kan altid ensidigt give instruks om, at Databehandleren skal standse videre behandling af de overladte personoplysninger.
11.2 Ændringerne anses først for gældende, fra ændringerne er implementeret.
11.3 Den Dataansvarlige kan med et rimeligt varsel til Databehandleren ændre bestemmelserne i Aftalen, hvis sådan ændring er nødvendig for at overholde gældende lovgivning.
11.4 I så fald skal Databehandleren sørge for at indarbejde tilsvarende ændringer i bestemmelserne i eventuelle aftaler med underdatabehandlere.

12. Varighed og ophør
Aftalen træder i kraft ved indgåelsen og løber, så længe det er relevant for Databehandlerens udførelse af aftalte opgaver og forpligtelser over for den Dataansvarlige, herunder så længe de praktiserende speciallægers brug af IT programmet Sentinel er aftalt mellem Regionernes Lønnings- og Takstnævn (RLTN) og Foreningen af Speciallæger (FAS) og disse parter er enige om, at dette sker via Databehandleren. Aftalen kan dog altid opsiges ensidigt af den Dataansvarlige.
12.1 Såfremt Aftalens ophør skyldes opsigelse fra den Dataansvarliges side, er Databehandler forpligtet til at slette alle personoplysninger, der er blevet behandlet på vegne af den Dataansvarlige, og bekræfte over for Dataansvarlig, at oplysningerne er slettet. Såfremt Aftalens ophør skyldes ændringer i Overenskomst om speciallægehjælp mellem RLTN og FAS - eller at overenskomstens parter måtte beslutte at anvise en an-den Databehandler end Sundhed.dk – påhviler det Dataansvarlig og Databehandler loyalt at fortsætte samarbejdet så længe det er nødvendigt for at indrette sig på overenskomstens nye indhold, og indtil der i givet fald kan indgås databehandleraftale mellem den Dataansvarlige speciallæge og en ny databehandler.
12.2 Efter sletning af Personoplysningerne må Databehandleren kun opbevare en kopi deraf, hvis det i henhold til EU-lovgivning eller EØS-medlemsstaternes nationale lovgivning er påkrævet, at Databehandleren opbevarer Personoplysningerne. I så fald skal Databehandleren underrette den Dataansvarlige derom, herunder med en henvisning til det juridiske grundlag for fortsat opbevaring. Den Dataansvarlige kan gøre indsigelse mod den fortsatte opbevaring af Personoplysningerne.
12.3 Hvis der efter Aftalens ophør opstår tvivl om, hvorvidt Databehandleren behørigt har slettet alle Personoplysningerne, kan den Dataansvarlige mod betaling af Databehandlerens omkostninger herved anmode om, at Databehandleren på den Dataansvarliges regning indhenter en revisorerklæring om, at Databehandleren ikke længere behandler Personoplysningerne.
12.4 Pkt. 5 (Databehandlerens bistand til den Dataansvarlige) og pkt. 10 (Påvisning af overholdelse, revisioner mv.) gælder i 18 måneder efter Aftalens ophør.

13. Lovvalg og værneting
13.1 Aftalen er underlagt dansk lovgivning.
13.2 Enhver tvist, som måtte opstå i forbindelse med Aftalen, herunder tvister vedrørende aftalens eksistens eller gyldighed, skal afgøres af domstolene.

14. Underskrifter
14.1 Aftalen underskrives elektronisk af Sundhed.dk som Databehandler og af Dataansvarlig speciallæge.

Bilag A Instruks med oplysninger om databehandlingen
1. Registrerede
1.1 Databehandleren behandler personoplysninger om følgende kategorier af registrerede ("Registrerede") på vegne af den Dataansvarlige og følgende type af personoplysninger (herefter benævnt " Personoplysninger") om de Registrerede på vegne af den Dataansvarlige:

Patienter:
Særlige kategorier af personoplysninger (følsomme og fortrolige oplysninger): Helbredsoplysninger og cpr.nr.
Generelle kategorier af personoplysninger: Navn

Speciallæger/klinikejere:
Generelle kategorier af personoplysninger: Navn, ydernummer, telefonnummer, mailadresse, oplysninger om journalsystem og andre ikkefølsomme oplysninger, der er nødvendige for Databehandlers udførelse af de aftalte opgaver

Ansatte i klinikken:
Generelle kategorier af personoplysninger: Navn, stilling og andre ikkefølsomme oplysninger, hvis de indgår i det datamateriale, der er nødvendigt for Databehandlers udførelse af de aftalte opgaver

2. Lovkrav
Relevant lovgivning er databeskyttelsesloven, sundhedsloven og lovgivning om kliniske kvalitetsdatabaser (pt. bkg nr. 585 af 28. maj 2018).

3. Underdatabehandlere
Databehandleren må gøre brug af underdatabehandlere uden forudgående specifik godkendelse fra den Dataansvarlige på de betingelser, der følger af Aftalens pkt. 8.

Følgende underdatabehandlere er godkendt på tidspunktet for Aftalens indgåelse:
Navn på underdatabehandler: CLOUDIO A/S
Adresse på underdatabehandler: Frode Jakobsens Plads 4, 4 sal, 2720 Vanløse
Land, hvor Personoplysningerne opbevares: Danmark
Formålet med overførslen til underdatabehandleren: CLOUDIO stiller servere og drift/support på disse til rådighed for Sentinel

Bilag B – Formål og supplerende instruks

Anvendelse af data til aftalte formål i Overenskomst om speciallægehjælp:
Det er i Overenskomst om speciallægehjælp mellem Regionernes Lønnings- og Takstnævn (RLTN) og Foreningen af Speciallæger (FAS) aftalt, at IT-programmet Sentinel skal anvendes til at samle data fra patientjournaler hos de praktiserende speciallæger med henblik på anvendelse af speciallægen selv, benchmarking, rapportering til kliniske kvalitetsdatabaser og videregivelse af diagnosekoder til regionerne, jf. nedenstående punkter 1-4.
Installationen af Sentinel foretages af den enkelte speciallæges systemleverandør.
Data fra patientjournaler indeholder personfølsomme oplysninger. Der er klar lovgivning om hvordan personfølsomme data må anvendes og til hvilke formål, og hvornår data skal være aggregerede og anonyme.
I dette bilag gives et overblik over, hvordan data via Sentinel må anvendes til de forskellige formål, der er aftalt i overenskomsten.
Der er i alle tilfælde tale om, at sundhed.dk fungerer som databehandler for speciallægen. Dvs. at der i juridisk forstand er tale om overladelse – og ikke videregivelse – af personoplysninger til sundhed.dk.
1. Anvendelse af speciallægen selv – personhenførbare oplysninger om egne patienter
Sentinel samler data fra speciallægens patientjournal og returnerer dem til speciallægen selv i struktureret form. Data indsamles og returneres i personhenførbar stand. De personhenførbare data må ikke videregives til andre, men udelukkende returneres til speciallægen selv. Formålet med denne anvendelse er at give speciallægen et systematiseret overblik over egne patienter og disses data, med henblik på kvalitetsudvikling og egen læring.

2. Benchmarking – aggregerede anonyme data
Benchmarking-data er aggregerede data, der skal give speciallægen mulighed for at holde egne data op imod data fra andre praksis inden for samme speciale. Benchmarking-data skal være anonyme, dvs. det må ikke være muligt at spore oplysningerne tilbage til den enkelte patient. Når data er samlet til benchmarking, er det gjort til statistiske data, der er

aggregeret, og datas tilknytning til den enkelte patient er fjernet uden mulighed for at genskabe den. Formålet med denne anvendelse er at kendskabet til sammenlignelige data skal kunne indgå i klinikkens kvalitetsarbejde.

3. Rapportering til landsdækkende kliniske kvalitetsdatabaser – personhenførbare oplysninger
Rapportering til godkendte landsdækkende kliniske kvalitetsdatabaser omfatter personhenførbare oplysninger, jf. den til enhver tid gældende lovgivning om kliniske kvalitetsdatabaser (pt. bkg. nr. 585 af 28. maj 2018).

4. Diagnosekoder fra den enkelte klinik til regionerne – ingen personhenførbare patientoplysninger
Regionerne skal i henhold til Overenskomst om speciallægehjælp modtage oplysning om diagnosekoder fra den enkelte klinik. Data må ikke indeholde personoplysninger, der kan spores tilbage til en konkret patient, men data kobles til en konkret klinik.

Når det er konstateret, at den Dataansvarlige regelmæssigt leverer data via Sentinel, fremsender Databehandler en orientering herom til regionen, som herefter udbetaler et i overenskomsten fastsat tilskud til de speciallæger, der ikke tidligere har modtaget tilskud for tilmelding til datafangst.
Yderligere formål:
Sundhed.dk (Databehandler) videregiver til eKVIS og Speciallægelandssamarbejdsudvalget oplysninger om den Dataansvarlige speciallæges opkobling til Sentinel, kontaktoplysninger og om deltagelse i rapportering til de i dette bilag beskrevne formål. Dette sker til implementeringsformål. Der vil ikke være tale om patientdata eller kliniske data. Aggregerede, ikke-personhenførbare data anvendes til statistikformål.

Bilag C - Sikkerhedsinstrukser
Databehandleren skal i forbindelse med behandling af Personoplysningerne som minimum træffe de nødvendige tekniske og organisatoriske sikkerhedsforanstaltninger, jf. Aftalens pkt. 6. Herudover skal Databehandleren træffe de nedenfor beskrevne tekniske og organisatoriske sikkerhedsforanstaltninger i forbindelse med behandling af Person-oplysningerne;
1. Standarder
1.1 Databehandleren skal efterleve principperne i ISO 27001 på relevante områder eller en i øvrigt anerkendt standard inden for IT-drift, i det omfang andet ikke fremgår af nærværende databehandleraftale.

2. Operationel sikkerhed
2.1 Databehandleren skal sikre:
(A) at det nødvendige og tilstrækkelige sikkerhedsniveau vedligeholdes og opretholdes, samt at eventuelle ændringer i Databehandlerens sikkerhedsforanstaltninger relevante for Personoplysningerne logges og dokumenteres,
(B) at ændringer og vedligeholdelse af Databehandlerens sikkerhedsforanstaltninger så vidt muligt ikke påvirker den Dataansvarliges forretning, herunder men ikke begrænset til it-systemer, netværk, forbindelser og svartider,
(C) at Databehandlerens eventuelle testmiljøer er tilstrækkelig afgrænset og i øvrigt sikret mod uautoriseret adgang,
(D) at Databehandlerens it-systemer og netværk er tilstrækkeligt sikret mod hacking og anden uautoriseret adgang,
(E) at Databehandleren gennemfører kontroller for at opdage og forhindre uautoriseret adgang, malware mv.
(F) at dennes interne operationelle sikkerhedsprocedurer og -manualer følges.

3. Fysisk sikkerhed
3.1 Databehandleren skal sikre sine fysiske lokaliteter, servere mv. mod uautoriseret adgang.
3.2 Databehandleren skal have interne sikkerhedsprocedurer der ved fjernelse, afhændelse eller genbrug af hardware sikrer, at den Dataansvarliges Personoplysninger ikke kompromitteres.

4. Backup
4.1 Databehandler skal foretage backup af indhentede data én gang i døgnet. Backup-overførslen skal være krypteret. Backup skal opbevares adskilt fra produktionsdata efter samme sikkerhedsniveau som produktionsdata.

5. Adgang til Personoplysninger
5.1 Databehandleren skal sikre, at kun relevante medarbejdere har adgang til de behandlede Personoplysninger.
5.2 Databehandleren skal efter den Dataansvarliges anmodning på ethvert tidspunkt kunne afgive en erklæring om hvilke personer, som har haft adgang til Personoplysningerne på vegne af Databehandleren.
5.3 Databehandleren skal sikre, at enhver person, der udfører arbejde for Databehandleren og får adgang til Personoplysningerne, kun behandler sådanne oplysninger efter den Dataansvarliges instruks, medmindre behandlingen er påkrævet i henhold til EU-lovgivningen eller EØS-medlemsstaternes nationale lovgivning.
5.4 Databehandleren skal sikre, at enhver person, der udfører arbejde for Databehandleren og får adgang til Personoplysningerne har oparbejdet tilstrækkeligt kendskab til korrekt håndtering af personoplysninger, og at de pågældende

medarbejdere er bekendt med de for Aftalen gældende sikkerhedskrav.

6. Hjemmearbejdsplads
6.1 Databehandling må kun foretages fra ad hoc arbejdspladser under anvendelse af medbragt godkendt konfigureret arbejdsstation (bærbar) fra sundhed.dk. Forbindelsen kan kun foretages via påkrævet VPN forbindelse med stærk godkendt kryptering (AES 256 bit) via sundhed.dk firewall under anvendelsen af 2 faktor autentifikation.

7. Logning
7.1 Databehandler foretager logning i overensstemmelse med lovgivningen og gældende branchestandarder.
7.2 Der skal foretages maskinel logning af alle anvendelser af personoplysninger. Loggen skal mindst indeholde oplysninger om tidspunkt, bruger, type af anvendelse og angivelse af den person, de anvendte oplysninger vedrører, eller det anvendte søgekriterium.
7.3 Bestemmelsen i pkt. 7.2 finder ikke anvendelse, hvis behandlingen af Personoplysninger sker ved afvikling af programmer, som foretager en foruddefineret massebehandling af Personoplysninger, eller hvis behandlingen sker med henblik på statistisk behandling, og identifikationsoplysningerne forinden enten er krypteret eller pseudonymiseret, f.eks. erstattet ved kodenummer eller lign. Der skal dog i begge tilfælde foretages maskinel logning af brugeren og tidspunktet for behandlingen.
7.4 Den Dataansvarlige kan på anmodning få de relevante logs udleveret fra Databehandleren.
7.5 Log opbevares i 6 måneder.

8. Samarbejde med myndigheder
8.1 Databehandleren samarbejder efter anmodning med Datatilsynet og eventuelle øvrige tilsynsmyndigheder i forbindelse med udførelsen af sådanne tilsynsmyndigheders opgaver. Databehandleren er herunder berettiget til at give Datatilsynet adgang til alle personoplysninger og oplysninger, der er nødvendige for at varetage Datatilsynets opgaver.
8.2 Databehandleren træffer de nødvendige foranstaltninger til at sikre overholdelse af en afgørelse fra Datatilsynet. Eventuelle ændringer i forhold til sikkerhedsniveau gennemføres som en ændring i henhold til denne Aftale. Databehandleren underretter på den datasvarliges vegne Datatilsynet om de foranstaltninger, der er truffet for at overholde afgørelsen.
8.3 Meddeler Datatilsynet Databehandleren påbud, skal Databehandleren efterkomme sådant påbud i overensstemmelse med den nærmere angivne måde og inden for den angivne frist.
8.4 Databehandleren har tilladelse til at tilgå den Dataansvarliges netværk og IT-systemer i det omfang det er nødvendigt i henhold til samarbejde med myndigheder (politi og efterretningstjeneste).