ClinicCare Databehandleraftale

Træder i kraft fra pr. 21. maj 2018

Indgået mellem den Dataansvarlig(e) i klinikken og Databehandleren:

ClinicCare Kliniksystemer
CVR-nr. 43 26 03 59
Gothersgade 12
DK-1123 København K

Den Dataansvarlige og Databehandleren er i hver for sig benævnt **"Part"** og under et **"Parterne"**

Parterne har indgået følgende databehandleraftale ("**Aftale**") vedrørende de data der håndteres på Databehandlerens server.

Indhold

1. Baggrund

1.1 Aftalen er indgået i forbindelse med Databehandlerens levering af serviceydelser i form af et kliniksystem til brug for behandling af patientoplysninger i den dataansvarliges klinik samt kommunikation og datatransmission til nødvendige tekniske sundhedstjenester via legale transportører og til legale modtagere (herefter omtalt som **"Serviceydelser**").

1.2 Aftalen regulerer forhold i relation til Serviceydelserne, gældende persondatalovgivning, jurisdiktion mv. mellem Parterne. Aftalen har forrang i tilfælde af uoverensstemmelser mellem Aftalen og alle andre aftaler mellem Parterne, herunder også aftalen om levering af serviceydelse (herefter omtalt som "Kontrakten"), såfremt den pågældende uoverensstemmelse omhandler et forhold vedrørende behandlingen af personoplysninger. Aftalen dækker alene ydelser, der er omfattet af Kontrakten.

1.3 Aftalen vedrører kun de data som Databehandleren behandler. Dvs. aftalen gælder kun de data, som Databehandleren har kontrol over på egen server. Hvis klinikken har installeret ClinicCare på egen server, er ClinicCare ikke Databehandler for disse data.

1.4 Enhver henvisning til Aftalen er også en henvisning til Aftalens Bilag.

1.5 Databehandleren er bekendt med Lov om behandling af personoplysninger af 31. maj 2000 ("**Persondataloven**"), 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 træder i kraft samtidig med/gælder sideløbende med Databeskyttelsesforordningen.

1.6 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 onlineidentifikator eller et eller flere elementer, der er særlige for denne fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sociale identitet" og/eller som termen er defineret i den for den Dataansvarlige gældende persondatalovgivning.

2.2 Aftalen finder anvendelse i forhold til Personoplysningerne, Registrerede, Formål og Behandlingsaktiviteter samt øvrige forhold og forpligtelser, der vedrører behandlingen, og som er defineret og anført i **Bilag A**.

2.3 Bilag A - B indgår i begge Parternes dokumentationsforpligtelser i henhold til persondatalovgivningen og skal altid afspejle de faktiske forhold.

2.4 Hvis Databehandleren bliver opmærksom på, at de faktiske oplysninger på et givent tidspunkt efter Aftalens ikrafttræden ikke stemmer overens med oplysningerne angivet i Bilag A f.eks. fordi flere kategorier end de i bilagene angivne er blevet overført til Databehandleren, skal Databehandleren straks fremsende en skriftlig meddelelse herom til den Dataansvarlige. Databehandleren har dog ikke pligt til at gennemgå de oplysninger, som behandles i systemet, med henblik på at sikre, at de faktiske oplysninger stemmer overens med oplysningerne angivet i Bilag A. Bilagene vil løbende blive opdateret i selve systemet og på Databehandlerens hjemmeside.

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, navnlig fsva. 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 alle systemer og registre efter instruks fra den Dataansvarlige. Databehandleren må dog behandle, herunder bl.a. isolere, flytte ogslette, 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. Alternativt 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 strengt fortrolige 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 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, 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

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 B**.

6.4 Parterne er enige om, at systemet der leveres som Serviceydelserne ikke skal ændres for at overholde de, i persondatalovgivningen indeholdte, krav til databeskyttelse gennem design og databeskyttelse gennem standardindstillinger, med mindre, der foretages sådanne grundlæggende og gennemgribende ændringer i Serviceydelserne, at kravet i Databeskyttelsesforordningens artikel 25 udløses. Den Dataansvarlige har i så fald krav på at der foretages ændringer for at overholde disse krav. Den Dataansvarlige har ansvaret for at indrette de processer, der udføres i systemet der leveres som Serviceydelser således, at de overholder persondatalovgivningens krav til databeskyttelse gennem design og databeskyttelse gennem standardindstillinger.

7. Sikkerhedsbrud

7.1 Definition

7.1.1 Ved et "Sikkerhedsbrud" forstås 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 Databehandleres 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

7.3.1 Databehandleren skal uden unødig forsinkelse underrette den Dataansvarlige ved mistanke om eller konstatering af et sikkerhedsbrud med betydning for Personoplysningerne.

7.3.2 Under hensyn til karakteren af behandlingen samt oplysningerne, der er tilgængelige for Databehandleren, skal Databehandleren efter et sikkerhedsbrud straks bistå den Dataansvarlige med at sikre overholdelse af den Dataansvarliges lovmæssige forpligtelser i forbindelse med underretning om sikkerhedsbrud til tilsynsmyndigheder og de Registrerede.

7.3.3 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 til, at den Dataansvarlige kan overholde lovbestemte forpligtelser. Databehandleren skal til dette formål levere følgende oplysninger på den Dataansvarliges anmodning:

(a) En beskrivelse af karakteren af sikkerhedsbruddet, herunder, hvis muligt, kategorierne og det omtrentlige antal af berørte Registrerede samt kategorierne og det omtrentlige antal af berørte registreringer med Personoplysninger

(b) Navn og kontaktoplysninger på databeskyttelsesrådgiveren eller anden kontaktperson, hvorfra yderligere oplysninger kan indhentes

(c) En beskrivelse af de sandsynlige samt de faktiske konsekvenser af sikkerhedsbruddet

(d) En beskrivelse af de foranstaltninger, som Databehandleren har truffet eller foreslår truffet for at håndtere Sikkerhedsbruddet, herunder, hvis det er relevant, foranstaltninger, der er foretaget for at begrænse dets mulige skadevirkninger.

Databehandleren skal desuden efter den Dataansvarliges anmodning uden unødig forsinkelse levere følgende oplysninger:

(e) En begrundet vurdering af, om Sikkerhedsbruddet sandsynligvis eller sandsynligvis ikke vil medføre en risiko for fysiske personers rettigheder og frihedsrettigheder

(f) En beskrivelse af de berørte systemer og processer

(g) En beskrivelse af årsagen til Sikkerhedsbruddet

(h) Tidspunktet for indtrædelsen af Sikkerhedsbruddet

(i) Varighed af sikkerhedsbruddet

(j) 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

(k) 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

(l) En oversigt over de tiltag, som Databehandleren allerede har iværksat, og i hvor høj grad tiltagene har begrænset eller afhjulpet Sikkerhedsbruddet

(m) En beskrivelse af hvilke foranstaltninger der kunne have forhindret Sikkerhedsbruddet.

7.3.4 Hvis og i det omfang det ikke er muligt at levere oplysningerne anført i pkt. 7.3.1 - 7.3.3 samlet, kan oplysningerne leveres gradvist. Den gradvise levering skal foregå uden unødige forsinkelser.

7.3.5 I det omfang en eller flere af de oplysninger, der er nævnt under pkt. 7.3.1 - 7.3.3, 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.

7.3.6 Hvis Sikkerhedsbruddet sker hos en underdatabehandler skal Databehandleren forestå kontakten til underdatabehandleren, medmindre andet aftales mellem Parterne.

7.4 Underretning af tredjemand

7.4.1 Hvis den Dataansvarlige efter persondatalovgivningen er forpligtet til at underrette enten myndighederne eller Registrerede om et sikkerhedsbrud, skal den Dataansvarlige afholde udgifter til at udarbejde og distribuere redegørelser eller offentlige udtalelser, der angiver både Databehandlerens og den Dataansvarliges ansvar i forbindelse med det formodede eller indtrufne sikkerhedsbrud, såfremt sikkerhedsbruddet alene skyldes den Dataansvarliges forhold.

7.4.2 Hvis Den Dataansvarlige efter persondatalovgivningen er forpligtet til at underrette enten myndighederne eller Registrerede om et sikkerhedsbrud, skal Databehandleren afholde udgifter til at udarbejde og distribuere redegørelser eller offentlige udtalelser, der angiver både Databehandlerens og den Dataansvarliges ansvar i forbindelse med det formodede eller indtrufne sikkerhedsbrud, såfremt sikkerhedsbruddet alene skyldes Databehandlerens forhold.

8. Information

8.1 Databehandleren skal straks informere den Dataansvarlige, hvis Databehandleren mener, at en instruks overtræder Databeskyttelsesforordningen, anden EU-ret eller medlemsstaternes nationale ret.

9. Honorar til Databehandlere

9.1 Databehandleren har krav på betaling efter medgået tid samt Databehandlerens øvrige omkostninger herved, for de ydelser der udføres efter Databehandleraftalen på den Dataansvarliges anmodning. Ydelserne kan omfatte, men er ikke begrænset til, assistance til den Dataansvarliges forpligtelser efter artikel 32 – 36, ændringer i Aftalen eller instruks, udlevering af oplysninger, bistand ved audit, bistand til Databeskyttelsesforordningens kapitel 3, bistand til ændringer der følger af nye risikovurderinger og konsekvensanalyser, så længe dette ikke beror på manglende levering af aftalte funktioner i de tekniske løsninger, der skal leveres af databehandleren. Dette gælder blandt andet:

1. Bistand til udlæsning, gennemgang og udredning af log i forbindelse med patientklagesager.

2. Bistand til kryptering eller anden yderligere sikring af databaser, netværk, servere og andet udstyr

der ikke er indeholdt i den Dataansvarliges kontrakt(er) med Databehandleren.

3. Bistand, ved anmodning fra den Dataansvarlige, til sletning af journaldata, såfremt den Dataansvarlige selv har teknisk tilgængelig mulighed for at kunne foretage sletningen.

9.2 For ydelser der ikke er omfattet af punkt 9.1 er Databehandleren dog ikke berettiget til vederlag i det omfang Databehandleren jf. lovgivningen er den direkte forpligtede part. Dette gælder kun for ydelser der ydes i relation til services og ydelser omfattet af Kontrakten jf. definitionen i punkt 1.2.

9.3 Vederlaget opgøres efter de aftalte timesatser i aftale(r)n(e) om levering af Serviceydelserne, og hvor der ikke er aftalt timesatser heri, da efter Leverandørens gældende timesatser, der dog ikke må overskride branchekutyme.

9.4 Databehandleren har uanset ovenstående ikke krav på betaling for assistance eller implementering af ændringer i det omfang, sådan assistance eller ændring er en direkte følge af Databehandlerens egen misligholdelse af denne Aftale.

10. Erstatningsansvar

10.1 Parternes ansvar under databehandleraftalen følger Kontraktens regulering. Hvis Kontrakten ikke regulerer ansvaret gælder nedenstående punkter. I forhold til ansvar over for tredjemand finder Databeskyttelsesforordningens art. 82 anvendelse.

10.2 Databehandleren er aldrig ansvarlig overfor den Dataansvarlige for indirekte tab, herunder men ikke begrænset til tab for følgeskade, tabt indtjening, driftstab, tabt goodwill, tab af data, tredjemands tab eller andet indirekte tab hos den Dataansvarlige eller tredjemand.

10.3 Uagtet årsagen til Databehandlerens eventuelle erstatningsansvar overfor den Data-ansvarlige, kan Databehandlerens samlede erstatningsansvar aldrig overstige et beløb svarende til det løbende abonnement, som den Dataansvarlige har betalt til Databehandleren i henhold til Kontrakten i en 6 måneders periode der går forud for den skadegørende handling eller undladelse. Såfremt Kontrakten ikke har været i kraft i 6 måneder på tidspunktet for den skadegørende handling eller undladelse, opgøres beløbet som det beløb der i henhold til Kontrakten er betalt som løbende vederlag henholdsvis burde være betalt som løbende abonnement i henhold til Kontrakten i Kontrakten første 6 måneder.

11. Underdatabehandlere

11.1 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 for 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.

11.2 Den Dataansvarlige har ved denne Aftales indgåelse godkendt underdatabehandleren/underdatabehandlerne anført i Bilag A. Databehandleren opdaterer løbende Bilag A med oplysninger om underdatabehandleren/underdatabehandlerne, der godkendes efter Aftalens indgåelse. Databehandleren skal sende det opdaterede Bilag A til den Dataansvarlige, for at denne kan overholde sine forpligtelser i henhold til gældende persondatalovgivning.

11.3 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 Aftalen, herunder at underdatabehandleren skal gennemføre passende tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen opfylder kravene i persondatalovgivningen.

11.4 Databehandleren er ansvarlig over for den Dataansvarlige for eventuelle underdatabehandlere på samme måde som for Databehandlerens egne handlinger og undladelser.

12. Placering af Personoplysninger

12.1 Databehandleren må 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.

12.2 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.

12.3 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.

12.4 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.

12.5 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.

13. Påvisning af overholdelse, revisioner mv.

13.1 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 persondatalovgivning samt gældende lovgivning om informationssikkerhed.

13.2 Databehandleren skal en gang årligt stille en rapport 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.

13.3 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.

14. Ændringer til Aftalen

14.1 Enhver ændring af Aftalen, herunder instruksen skal ske efter ændringsproceduren i Kontrakten, idet den Dataansvarlige dog altid ensidigt kan give instruks om, at Databehandleren skal standse videre behandling af de overladte personoplysninger.

14.2 Databehandleren har krav på betaling af omkostninger forbundet med ændringer i overensstemmelse med pkt. 9.

14.3 Ændringerne anses først for gældende, fra ændringerne er implementeret.

14.4 Databehandleren kan afslå en ændring. Databehandleren skal herefter ophøre med videre behandling af den Dataansvarliges personoplysninger og enten slette eller tilbagelevere oplysningerne efter den Dataansvarliges valg og i overensstemmelse med punkt 15 nedenfor.

14.5 Den Dataansvarlige kan med et rimeligt varsel til Databehandleren ændre bestemmelserne i Aftalen, hvis sådan ændring er nødvendig for at overholde gældende lovgivning.

14.6 I så fald skal Databehandleren sørge for at indarbejde tilsvarende ændringer i bestemmelserne i eventuelle aftaler med underdatabehandlere.

15. Varighed og ophør

15.1 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 under Kontrakten.

15.2 Databehandleren skal ved ophør af leveringen af Serviceydelser og Aftalen (det seneste af disse tidspunkter) på anmodning fra den Dataansvarlige slette eller tilbagelevere alle eksisterende eksemplarer af Personoplysningerne på et medie valgt af den Dataansvarlige og slette alle eksisterende eksemplarer af Personoplysningerne.

15.3 Efter tilbagelevering af Personoplysningerne til den Dataansvarlige/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.

15.4 Hvis der efter Aftalens ophør opstår tvivl om, hvorvidt Databehandleren behørigt har slettet alle Personoplysninger, 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 Personoplysninger.

15.5 Pkt. 5 (Databehandlerens bistand til den Dataansvarlige) og pkt. 13 (Påvisning af overholdelse, revisioner mv.) gælder i 18 måneder efter Aftalens ophør.

16. Lovvalg og værneting

16.1 Aftalen er underlagt dansk lovgivning.

16.2 Enhver tvist, som måtte opstå i forbindelse med Aftalen, herunder tvister vedrørende aftalens eksistens eller gyldighed, skal afgøres af domstolene.

17. Underskrifter

17.1 Aftalen er underskrevet nedenfor af Databehandler. Pr. den 1. maj 2018, kan man i kliniksystemet elektronisk tiltræde aftalen. Klinikken skal opbevare udskrevet kopi af aftalen.

17.2 Databehandleren oplyser, at underskrifterne er juridisk bindende for Databehandleren.

For ClinicCare, København. 23. april 2018

Anders Kjærulff

[Navn]

For klinikken,_____

[Navn]

Bilag A - Oplysninger om databehandlingen

Version 1: 1. maj 2018

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	Helbredsoplysninger, race eller etnisk oprindelse seksuelle forhold eller seksuel orientering politisk-, religiøs-, filosofisk overbevisning fagforeningsmæssigt tilhørsforhold oplysninger om straf eller lovovertrædelser samt Genetiske eller biometriske oplysninger. Sociale/funktionelle problemer, medicinforbrug, undersøgelser/laboratoriesvar, sygefravær Billediagnostisk materiale. Værgeoplysninger.
Generelle kategorier af personoplysninger	Navn, telefonnummer, postadresse, fødselsdato, mailadresse, brugerkonto SoMe, cpr.nr, familieforhold, bolig, beskæftigelse/stilling, køn, Foto ID, Betalingsforhold, medlemsnummer, bevilling fra firma-, forenings- og forsikringsordninger. Tilfredshedsundersøgelser, administrative procesdata (mødetidspunkt, aflysninger, ventetider), kvalitetsindikatorer.

	Klinikmedarbejdere
Særlige kategorier af personoplysninger	Oplysning om status vedr. hemmeligt navn, telefonnummer og/eller adresse.
Generelle kategorier af personoplysninger	Navn, telefonnumre, postadresse, fødselsdato, CPR, mailadresse, systemlog udvisende brug af system, stilling, aflønningsoplysninger, fraværsoplysninger, fagkompetencer, Foto ID, IP-adresse, ydernummer, autorisationskoder, CVR EAN, lokationsnummer.

	Medarbejdere hos eksterne partnere (kommune/forsikring etc)
Generelle kategorier af personoplysninger	Navn, telefonnumre, mailadresse, stilling, CVR/EAN-numre

2. Formål

2.1 Databehandlerens behandling af Personoplysninger for den Dataansvarlige sker til følgende formål:

17.3 Levering af de aftalte it-ydelser, herunder levering af kliniksystem samt kommunikation og datatransmission til nødvendige tekniske sundhedstjenester via legale transportører og til legale modtagere.

3. Databehandlingsaktiviteter/databehandlingens karakter

3.1 Databehandlerens behandling af Personoplysninger for den Dataansvarlige sker i overensstemmelse med Kontrakten om omfatter bl.a., herunder men ikke begrænset til. følgende aktiviteter:

- Ved at opbevare Personoplysninger og sikre systemers tilgængelighed, integritet og fortrolighed
- Ved at yde remote service til den Dataansvarliges brugere af kliniksystem
- Ved at formidle Personoplysninger til tredjeparter efter den Dataansvarliges instruks
- Sletning

4. Modtagere

4.1 Databehandleren må ud over eventuelle underdatabehandlere videregive Personoplysninger til modtagere, som den Dataansvarlige er forpligtet til at videregive personoplysninger til. Den Dataansvarlige er ansvarlig for, at overholde den til enhver tid gældende persondatalovgivning i forhold til de personoplysninger, som overlades til Databehandlerens behandling med henblik på videregivelse. Bilag D indeholder liste over dataunderbehandlere og interessenter, som databehandleren videregiver personoplysninger til.

4.2 Den Dataansvarlige er forpligtet til at vedligeholde en liste over disse modtagere.

4.3 Databehandleren kan ikke – uden den dataansvarliges specifikke og skriftlige godkendelse – anvende den enkelte underdatabehandler til en ”anden” behandling and aftalt.

Bilag B - 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 Personoplysningerne;

Databehandler, er ikke ansvarlig for behandling af de kopier af oplysninger, som Databehandler selv måtte tage, til egne servere, computere, eller andre media.

1. Standarder

1.1 Databehandleren skal efterleve principperne i ISO 27001 på relevante områder eller en i øvrigt anerkendt standard indenfor 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 svindel, malware mv., og

(F) at dennes interne operationelle sikkerhedsprocedurer og -manualer følges.

(G) at data aldrig placeres på servere uden for EU/EØS.

(H) at i tilfælde af en underleverandørs konkurs/større udfald, kan databehandling fortsætte i reserver hosting center.

2.2 Dataansvarlige skal sikre;

(A) at Databehandlerens it-systemer og netværk er tilstrækkeligt sikret mod hacking og anden uautoriseret adgang,

(B) at Databehandleren gennemfører kontroller for at opdage og forhindre svindel, malware mv., og

(C) at dennes interne operationelle sikkerhedsprocedurer og -manualer følges. Herunder, at man har læst de guider, som Databehandler udgiver omkring sikkerhed, og følger disses anvisninger.

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 Databehandleren skal foretage backup af Personoplysningerne samt teknisk test af backup, i det omfang backup er en del af Kontrakten.

4.2 Såfremt det er en del af Kontrakten, vil Databehandleren herefter én gang i døgnet tage en backup af den Dataansvarliges oplysninger i journalsystemet. Backup-overførslen skal være krypteret. Backup skal opbevares i et aflåst område i en anden bygning end hvor produktionsserveren fysisk er placeret. Backup gemmes i henhold til den i Kontrakten definerede periode.

4.3 Databehandleren stiller en erklæring om backup og teknisk test af backup til rådighed for den Dataansvarlige.

5. Sletteprocedure

5.1 Den Dataansvarlige kan selv i systemet fastsætte en regel for, hvornår systemet skal slette data. Patienten kan også anmode om sletning af data. Databehandleren kan i en periode i op til 10 år, gendanne slettede data.

5.2 I tilfælde af ophør af kundeforhold, herunder også ved manglende betaling af abonnement, vil data blive slettet efter overførsel til evt. ny leverandør. Hvis der ikke findes en ny leverandør, kan Databehandler tilbyde, at opbevare en kopi af data i 10 år.

6. Adgang til Personoplysninger

6.1 Databehandleren skal sikre, at kun relevante medarbejdere har adgang til de behandlede Personoplysninger.

6.2 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.

6.3 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. Specielt skal det gælde, at hvis systemudvikling outsources til lande uden for EU, skal pågældende leverandør tiltræde reglerne i henhold til EU-lovgivningen.

6.4 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.

6.5 Databehandleren skal tilstræbe, at medarbejdere kun i det omfang, at det er nødvendigt, får adgang til personhenførbare oplysninger.

6.6 Databehandleren sikre, at medarbejdere der sidder i 1st line support hos ClinicCare, ikke har direkte adgang til databaserne. Det betyder, at de eksempelvis ikke kan trække data ud af systemerne.

6.7 I systemerne ClinicCare Web, ClinicCare Windows, ClinicCare SQL er journaldata opbevaret krypteret, hvilket betyder at IT-support medarbejdere hos Databehandleren ikke kan læse journalerne. Hvis en opgave kræver, at en medarbejder skal åbne en journal, sker der en logning.

7. Logning

7.1 Databehandler foretager logning i overensstemmelse med lovgivningen og gældende branchestandarder.

7.2 Der skal foretages logning af alle afviste adgangsforsøg. Hvis der inden for en periode på [24 timer] er registreret højst [5] på hinanden følgende afviste adgangsforsøg fra samme bruger, skal der blokeres for yderligere forsøg. Adgangen må først åbnes, når årsagen er klarlagt og dokumenteret.

7.3 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. Af bilag C fremgår hvad der logges i systemet. Databehandler, forbeholder sig ret til, at udvide hvad der logges.

7.4 Det tilstræbes at Databehandler selv kan få adgang til alle logs via systemet. Den Dataansvarlige kan på anmodning få udleveret alle logs, der har relation til klinikken.

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 personoplysniger og oplysninger, der er nødvendige for at varetage Datatilsynets opgaver.

Efter Databehandlerens valg træffer enten den Dataansvarlige eller Databehandleren 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. Den Dataansvarlige underretter Datatilsynet om de foranstaltninger, der er truffet for at overholde afgørelsen.

Meddeler Datatilsynet Databehandleren påbud, skal Databehandleren efterkomme sådant påbud i overensstemmelse med den nærmere angivne måde og inden for den angivne frist.

9. Den Dataansvarliges tilsyn med behandlingen af data hos databehandleren handlere,

9.1 Den dataansvarlige eller en repræsentant for den dataansvarlige kan efter aftale, med et varsel på mindst 30 dage, hvert år i august/september foretage et fysisk tilsyn vedrørende overholdelsen af denne databehandleraftale hos databehandleren.

9.2 Den dataansvarliges eventuelle udgifter i forbindelse med et fysisk tilsyn afholdes af den data-ansvarlige selv. Databehandleren er berettiget til at fakturere med gået i forbindelse med kontrolbesøget.

10. Databehandlere, der har adgang til den Dataansvarliges IT-systemer og/eller den Dataansvarlige fysiske bygninger mv.

10.1 Databehandlere, der har adgang til den Dataansvarliges IT-systemer og/eller fysiske bygninger, skal ud over sikkerhedskravene i dette underbilag B, endvidere overholde de af dette punkt 5 omfattede sikkerhedskrav.

10.2 Databehandleren har tilladelse til at tilgå den Dataansvarliges netværk og IT-systemer i det omfang det er nødvendigt i henhold til Kontrakten. Dette sker via legale og sikkerhedsgodkendte værktøjer og kanaler, jf bilag B.

Bilag C – Hvad logges

Flg. hændelser I "loggen" med tidspunkt samt brugerinitial (nogle af hændelser er ikke relevante i alle systemer)

50	Funktion: Send og modtag	810	Aftale oprettet
53	Funktion: CPRnr-opslag	813	Aftale slettet
54	Funktion: Computer-dato ændret	910	Medicinering/vacc oprettet
55	Patient identitet verificeret	911	Medicinering/vacc ændret
80	Ajourfør medicinkort	912	Medicinering vist
81	Markeret medicinkort 'Ikke ajourført'	913	Medicinering slettet/seponeret
95	På vegne af hændelse	916	Medicinering ajourført
97	Journaladgang tilsidesat	1210	Ekons: Oprettet
98	Rettighed ændret	1213	Ekons: slettet
99	Samtykke tilsidesat	1214	Ekons: sendt
110	Patient www login	1216	Ekons: besvaret
111	Patient www formange loginforsøg	1310	Recept oprettet
112	Patient www Booking	1313	Recept slettet
150	Login	1314	Recept sendt
151	Login fejlforsøg	1410	Henvisning oprettet
154	Logout	1413	Henvisning slettet
156	Ændret kendeord	1414	Henvisning sendt
157	Bruger låst (for mange forsøg)	1512	Udskrift vist/læst (+kriterie for udskrift)
158	Kendeord nulstillet		
212	Stamkort vist		
213	Stamkort slettet		
214	Stamkort arkiveret		
612	Journal vist		
613	Journal slettet		
615	Journal modtaget		
710	Dokument oprettet		
713	Dokument slettet		

Bilag D - Dataflow, herunder anvendte underdatabehandlere

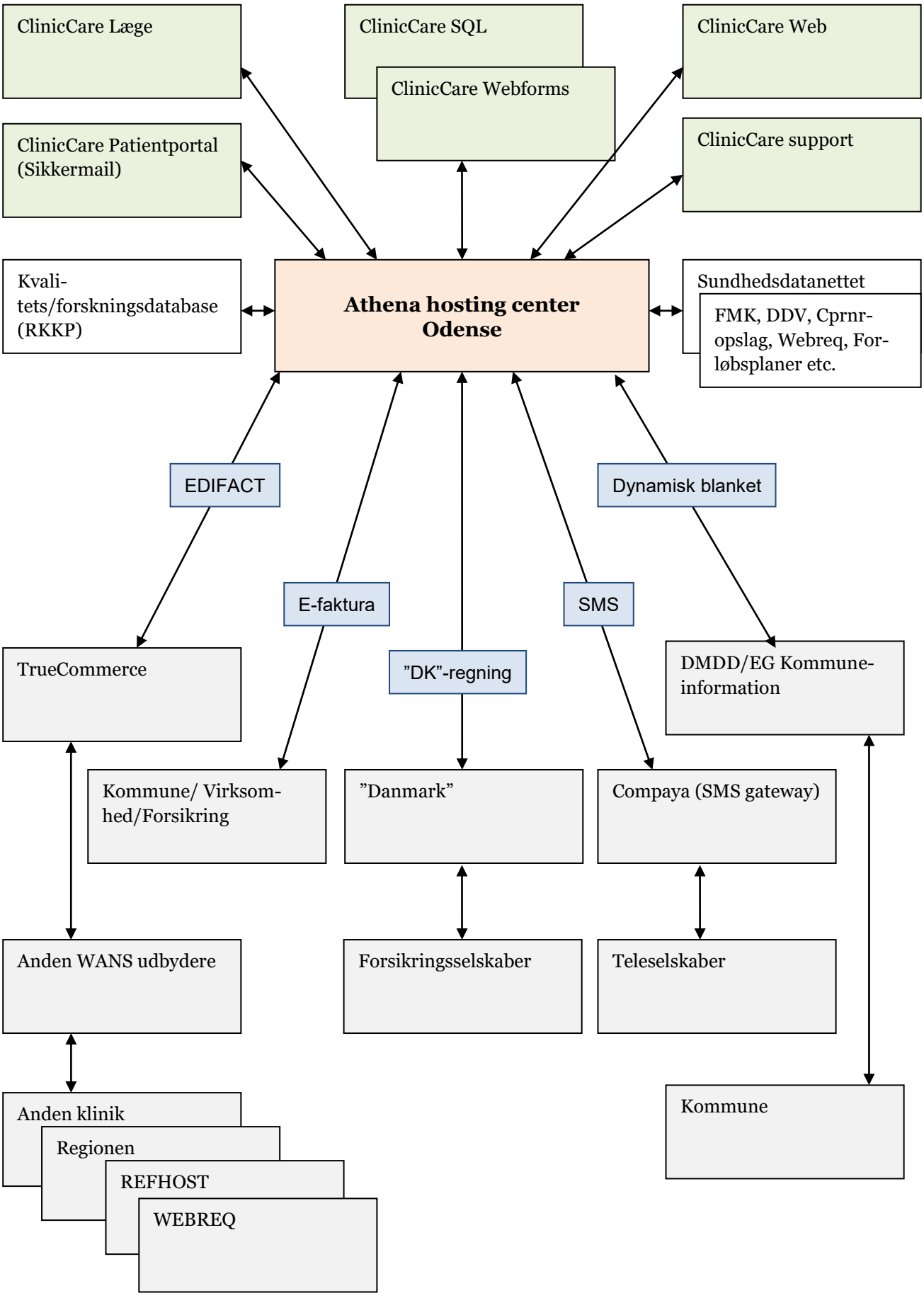
Navn	CVR	Beskrivelse af handling
Athena it-group a/s Munkerisvej 1 DK-5230 Odense M	DK19560201	Underdataleverandør: Hoster database og sikre backup af data til SQL-løsningerne (ClinicCare Læge, ClinicCare SQL, ClinicCare Web, ClinicCare Webforms). Håndtere sikkerhed overfor interessenter.
COMPAYA A/S Palægade 4, 2. tv. Dk-1261 København K	DK28119305	Håndtere forsendelse af SMS. Patientens mobiltelefonnummer samt den af klinikken definerede tekst fremsendes.
Netsite A/S Bredgade 30 DK-1260 København K	DK25233476	Underdataleverandør: Er reserve hosting center. Anvendes i en overgangsperiode i det tilfælde, at adgangen til Athena-hosting center helt afbrydes og ophøre.
NordicBackup A/S Naverland 2, 3. sal DK-2600 Glostrup	DK28119305	Underdataleverandør: Anvendes til backup af data placeret der ikke er inkluderet under nævnte ”Athena” ovenfor. Dvs. anvendes af klinikker, der ikke anvender ClinicCare Læge, ClinicCare SQL, eller ClinicCare Web.
TrueCommerce Denmark Banevænget 13 DK-3460 Birkerød	DK33776349	Underdataleverandør: Hertil videresendes og modtage EDIFACT, indeholdende journaloplysninger, samt flg. oplysninger på patient: CPR, Navn, adresse, telefon, e-mail.

Videregivelse af oplysninger sker til flg. interessenter (der skal ikke indgås databehandleraftale med disse):

Navn		Beskrivelse af handling
Sygeforsikringen ”Danmark”		Hertil videresendes ”Danmark”-regninger, CPR, behandlingsdato, ydelseskode, patientandel.
Sygesikring (regionen)		Hertil videresendes sygesikrings-regninger, CPR, behandlingsdato, ydelseskode, sygesikringsandel, henvisningsårsag, henviser
Given modtager af OIO-faktura		Hertil videresendes E-faktura (OIOUBL) indeholdende ydelsesoplysning (behandlingsdato, ydelseskode, evt. patient- og sygesikringsandel, evt. behandlingsområde). Hvis der fremsendes oplysninger om selve patienten, så fremsendes der kun CPR og navn.

Udover ovennævnte liste vil klinikken have en række samarbejdspartnere, som der udveksle oplysninger med, Der skal ikke indgås databehandleraftale med disse.

Næste side viser skematisk oversigt over datastrømme.


ClinicCare Læge
ClinicCare SQL
ClinicCare Webforms
ClinicCare Web
ClinicCare Patientportal (Sikkermail)
ClinicCare support
Kvali-tets/forskningsdatabase (RKKP)
Athena hosting center Odense
Sundhedsdatanettet
FMK, DDV, Cprnr-opslag, Webreq, For-løbsplaner etc.
EDIFACT
Dynamisk blanket
E-faktura
SMS
TrueCommerce
"DK"-regning
DMDD/EG Kommune-information
Kommune/ Virksom-hed/Forsikring
"Danmark"
Compaya (SMS gateway)
Anden WANS udbydere
Forsikringsselskaber
Teleselskaber
Anden klinik
Regionen
REFHOST
WEBREQ
Kommune