SYNLAB
MEDICAL DIGITAL SERVICES

Databehandleraftale

vedr. brug af WebReq (WBRQ)

Version 1.4, 2. januar 2023

Indhold

1. Baggrund for databehandleraftalen

1.1 Databehandleren er ansvarlig for udvikling og drift af IT-systemerne WebReq (WR) og Web-Patient (WP), der gør det muligt at stille relevante oplysninger til rådighed for parterne på sundhedsområdet.

1.2 Formålet med Databehandleraftalen er at regulere hvordan og til hvilket formål, Databehandleren skal behandle Personoplysninger på vegne af den Dataansvarlige samt at sikre, at den Dataansvarliges Personoplysninger behandles i henhold til den Dataansvarliges retningslinjer og instrukser samt gældende databeskyttelseslovgivning.

1.3 Aftalen er udformet med henblik på parternes efterlevelse af artikel 28, stk. 3, i 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 og om ophævelse af direktiv 95/46/EF ("Databeskyttelsesforordningen"), samt parternes efterlevelse af Sundhedsloven med tilhørende bekendtgørelser.

1.4 Nærværende databehandleraftale har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne.

1.5 Til nærværende Databehandleraftale hører A, bilag der fungerer som en integreret del af aftalen.

1.6 I henhold til Artikel 28 i Databeskyttelsesforordningen opbevares Databehandleraftalen skriftligt, herunder elektronisk af begge parter.

1.7 Nærværende databehandleraftaler erstatter samtlige tidligere Databehandleraftaler mellem parterne.

2. Forpligtelser og rettigheder for den dataansvarlige

2.1 Den Dataansvarlige har, overfor omverdenen (herunder den registrerede) som udgangspunkt, ansvaret for at behandlingen af Personoplysninger lever op til kravene i Databeskyttelsesforordningen og Databeskyttelsesloven der træder i kraft 25. maj 2018.

2.2 Den Dataansvarlige, er ved brug af de tjenester som Databehandler stiller til rådighed i henhold til Aftalen, forpligtet til at behandle Personoplysninger i overensstemmelse med bestemmelserne i gældende lovgivning om behandling af personoplysninger.

2.3 Den Dataansvarlige har derfor både rettighederne og forpligtelserne til at træffe beslutninger om, til hvilke formål og med hvilke hjælpemidler der må foretages behandling.

2.4 Den Dataansvarlige er blandt andet ansvarlig for, at der foreligger hjemmel til den

behandling, som Databehandleren instrueres i at foretage.

2.5 Da de primære samarbejdsorganer og kommunikationspartnere ift. de enkelte dataejeres interesser er henholdsvis Praktiserende Lægers Organisation (PLO), WR og WP Brugergrupperne og MedCom, vil de generelle instrukser vedr. databehandlingen, som SYNLAB Medical Digital Services følger, være aftalt i disse samarbejdsfora.

3. Databehandlerens forpligtelser

3.1 Databehandleren behandler Personoplysninger på vegne af og på baggrund af instrukser fra den Dataansvarlige.

3.2 Databehandleraftalens Bilag A indeholder nærmere oplysninger om behandlingen, herunder om behandlingens formål og karakter, typen af personoplysninger, kategorierne af registrerede og varighed af behandlingen.

3.3 Databehandleren behandler tillige Personoplysninger i det omfang det kræves i henhold til gældende EU-ret eller national ret, som databehandleren er underlagt; i så fald underretter databehandleren den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser, jf. art 28, stk. 3, litra a Persondataforordningen.

3.4 Databehandleren skal ligeledes overholde de til enhver tid gældende regler, der følger af Sundhedsloven med tilhørende bekendtgørelser.

4. Fortrolighed

4.1 Databehandleren skal sikre, at Personoplysningerne er underlagt fortrolighed, integritet og tilgængelighed i henhold til gældende lovgivning om behandling af personoplysninger.

4.2 Databehandleren skal sikre, at kun de personer, der aktuelt er autoriseret hertil, har adgang til de personoplysninger, der behandles på vegne af den dataansvarlige. Adgangen til oplysningerne skal derfor straks lukkes ned, hvis autorisationen fratages eller udløber.

4.3 Der må alene autoriseres personer, for hvem det er nødvendigt at have adgang til personoplysningerne for at kunne opfylde databehandlerens forpligtelser overfor den dataansvarlige.

4.4 Databehandleren sikrer, at de personer, der er autoriseret til at behandle Personoplysninger på vegne af den Dataansvarlige, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.

5. Behandlingssikkerhed

5.1 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.

5.2 Databehandleren skal iværksætte alle foranstaltninger, i henhold til databeskyttelsesforordningens artikel 32, hvoraf det bl.a. fremgår, at der under hensyntagen til det aktuelle niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder skal gennemføres passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici.

5.3 Ovenstående forpligtelse indebærer, at databehandleren skal foretage en risikovurdering, og herefter gennemføre foranstaltninger for at imødegå identificerede risici. Der kan herunder bl.a., alt efter hvad der er relevant, være tale om følgende foranstaltninger:

- Pseudonymisering og kryptering af personoplysninger
- Evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og – tjenester
- Evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse
- En procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed

5.4 Sikkerhedsforanstaltninger, der etableres hos databehandleren, skal være i overensstemmelse med ISO27001 standard for informationssikkerhed.

5.5 Databehandleren er underlagt kravene i Sikkerhedsbekendtgørelsen (nr. 528 af 15. juni 2000 med senere ændringer)

6. Underretning om brud på datasikkerheden

6.1 Databehandler underretter uden unødig forsinkelse den Dataansvarlige efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos Databehandleren eller en eventuel underdatabehandler.

6.2 Databehandleren skal under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for denne – bistå den dataansvarlige med at foretage anmeldelse af bruddet til tilsynsmyndigheden.

7. Underdatabehandlere

7.1 Databehandleren skal opfylde de betingelser, der er omhandlet i databeskyttelsesforordningens artikel 28, stk. 2 og 4, for at gøre brug af en anden databehandler (underdatabehandler).

7.2 Databehandleren må således ikke gøre brug af en anden databehandler (underdatabehandler) til opfyldelse af databehandleraftalen uden forudgående specifik eller generel skriftlig godkendelse fra den dataansvarlige. Dog må databehandleren gøre brug af de gængse nationale certificerede infrastrukturkomponenter på sundhedsdatanettet som VANS, CPR-opslag mv., som tillige benyttes af den dataansvarlige.

7.3 Ved indgåelse af denne Databehandleraftaler meddeler den dataansvarlige generel godkendelse til at databehandleren kan gøre brug af de gængse nationale certificerede infrastrukturkomponenter på sundhedsdatanettet som VANS, CPR-opslag mv., som tillige benyttes af den dataansvarlige, til at databehandleren kan gøre brug af hosting leverandører, som leverer drift og backup af servere og til at databehandleren kan gøre brug af software virksomheder og/eller freelancere, som hjælper med at udvikle og videreudvikle produkterne.

7.4 Når databehandleren har den dataansvarliges godkendelse til at gøre brug af en underdatabehandler, sørger databehandleren for at pålægge underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er fastsat i denne databehandleraftale, gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, hvorved der navnlig stilles de fornødne garantier for, at underdatabehandleren vil gennemføre de passende tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen opfylder kravene i databeskyttelsesforordningen.

7.5 Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver databehandleren fuldt ansvarlig over for den dataansvarlige for opfyldelsen af under-databehandlerens forpligtelser.

8. Bistand til den dataansvarlige

8.1 Databehandleren skal bistå med at sikre overholdelse af forpligtelserne i medfør af artikel 32-36 under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren.

8.2 Databehandleren skal bistå den dataansvarlige, ved hjælp af passende tekniske og organisatoriske foranstaltninger, med opfyldelse af den dataansvarliges forpligtelser til at besvare anmodninger om udøvelse af de registreredes rettigheder herunder, men ikke begrænset til:

- ret til at få indsigt

- ret til berigtigelse
- ret til sletning
- ret til begrænsning af behandling
- ret til dataportabilitet
- ret til indsigelse

9. Sletning og/eller tilbagelevering af personoplysninger

9.1 Ved ophør af tjenesterne vedrørende behandling forpligtes databehandleren til, efter den dataansvarliges valg, at slette eller tilbagelevere alle personoplysninger til den dataansvarlige, samt at slette eksisterende kopier, medmindre EU-retten eller national ret foreskriver opbevaring af personoplysningerne.

10. Revision og tilsyn

10.1 Databehandleren stiller alle oplysninger, der er nødvendige for at påvise databehandlerens overholdelse af databeskyttelsesforordningens artikel 28 og denne aftale, til rådighed for den dataansvarlige og giver mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af den dataansvarlige eller en anden revisor, som er bemyndiget af den dataansvarlige.

10.2 Databehandleren er forpligtet til at give myndigheder, der efter den til enhver tid gældende lovgivning har adgang til den dataansvarliges og databehandlerens faciliteter, eller repræsentanter, der optræder på myndighedens vegne, adgang til databehandlerens fysiske faciliteter mod behørig legitimation.

11. Ikrafttræden og ophør

11.1 Databehandleraftalen træder i kraft ved den dataansvarliges accept i WebReq.

11.2 Aftalen er gældende, så længe behandlingen består. Databehandleraftalen forbliver i kraft frem til behandlingens ophør og oplysningernes sletning hos databehandleren og eventuelle underdatabehandlere.

11.3 Databehandleraftalen gælder indtil den opsiges eller bortfalder efter aftale mellem parterne.

Oplysninger om behandlingen

Formålet med behandlingen

Formålet med databehandlingen i systemerne WebReq og Web-Patient er håndtering af bestillingsprocessen af laboratorieydelser og hjemmemålinger af patient eller borger sikker

og fortrolig udveksling af helbredsoplysninger i forbindelse med forsikringsattester, mellem læge, patient og forsikringsselskab

Karakteren af behandlingen

Data i bestillingsprocessen modtages dels via systemkaldet fra lægesystemet – eller indtastning, hvis bestilleren ikke har system - og behandles således at optimal bestilling kan foretages og udskrives af brugeren. Data videresendes via Sundhedsvæsenets gængse sikre kanaler (VANS, Sundhedsdatanet eller dedikerede VPN-tunneler).

Data opbevares tidsbegrænset og slettes herefter i systemet. Slettetidspunkt fastlægges af WR og WP-brugergrupperne.

Typen af personoplysninger

De personhenførbare data, der kan indgå i bestillingsprocessen, er:

CPR-nummer, navn, e-mailadresse, telefonnummer, adresse samt sundheds- og helbredsoplysninger.

Kategorierne af registrerede

Patienter og borgere i Danmark.

Generelt

Den konkrete databehandling af dataejerens data vil til enhver tid være dokumenteret og tilgængelig på SYNLAB Medical Digital Services' hjemmeside.

WR og WP og dermed omfanget af databehandlingen er i stadig udvikling.

Dataejerens interesser varetages i den forbindelse gennem de primære samarbejdsorganer, WR og WP Brugergrupperne. I disse fora defineres og prioriteres udviklingsopgaverne af interessenterne bag WebReq (WR) og Web-Patient (WP), dvs. PLO, MedCom, Laboratorier, Regioner, Klinik- og laboratoriefagligt personale.