Bilaga 1

Instruktioner för databehandlingen

I denna bilaga ges översiktlig information om de personuppgifter som Personuppgiftsansvarig kan komma att behandla inom ramen för Huvudavtalet och som Personuppgiftsbiträdet kan komma att biträda. Bilagan innehåller även information om exempelvis ändamål, behandlingsaktiviteter, plats för behandling och informationssäkerhet för Personuppgiftsbiträdets behandling av sådana personuppgifter.

Ändamål

Att uppfylla Personuppgiftsbiträdets åtaganden enligt Huvudavtalet.

Allmänt om personuppgifter i Personuppgiftsbiträdets system

Personuppgiftsbiträdet innehar generellt rättigheterna till de system Personuppgiftsbiträdet tillhandahåller till Personuppgiftsansvarig, med de eventuella avvikelser som förekommer i Huvudavtalet. Personuppgiftsbiträdets utgångspunkt är att alla uppgifter som den Personuppgiftsansvarige, eller någon annan på uppdrag av den Personuppgiftsansvarige, för in i systemet, avseende exempelvis användare och patienter, ägs av den Personuppgiftsansvarige. Att den Personuppgiftsansvarige registrerar uppgifter i något av Personuppgiftsbiträdets system innebär därmed inte automatiskt att Personuppgiftsbiträdet blir biträde till sådan behandling, utan Personuppgiftsbiträdet utgör endast biträde i de fall där Personuppgiftsbiträdet på något sätt behandlar införda personuppgifter. Personuppgiftsbiträdet genomför behandling för sina kunder enligt respektive Huvudavtal främst i de fall Personuppgiftsbiträdet tillhandahåller drift av systemet för Personuppgiftsansvarig, tillhandahåller kommunikation av personuppgifter från och till andra system (exempelvis nationella tjänster) samt i de fall personuppgifter förekommer i supportärenden eller vid konsultuppdrag (exempelvis migreringar, registrering av uppgifter på uppdrag av Personuppgiftsansvarig, rättningar enlig instruktion från Personuppgiftsansvarig).

Personuppgiftsansvarig är alltid ansvarig för att insamling, registrering av uppgifter, information till registrerad person, raderingsrutiner och andra legala krav som ställs på insamling och hantering av personuppgifterna genomförs enligt tillämpliga lagar, förordningar och föreskrifter. Personuppgiftsbiträdet ansvarar endast för att den behandling som Personuppgiftsbiträdet genomför enligt Huvudavtalet sker i enlighet med detta Avtal.

Kategorier av registrerade

Alla kategorier av registrerade som den Personuppgiftsansvarige kan komma att registrera/förmedla, vilket främst är;

patienter/elever/anställda/brukare/andra personer som nyttjar eller har rätt att nyttja kundens tjänster ("Vårdtagare"), Vårdtagares närstående och andra kontakter, anställd personal (användare) hos kunden, konsulter/personal hos underleverantörer, vårdpersonal eller andra personer som inte är anställda hos kunden men som har koppling till patienten på annat sätt

(ex. remissavsändare/mottagare på annan vårdenhet/laboratorium, annan skolpersonal, personal hos andra myndigheter eller liknande).

Kategorier av uppgifter

För anställda/konsulter hos Personuppgiftsansvarig (notera att inte alla uppgifter är tillämpliga för alla anställda/konsulter);

namn och kontaktuppgifter, personnummer, yrkesroll, kompetens, koder kopplade till personen (exempelvis HSA-ID, anställningsnummer, förskrivarkod eller dyl.), behörigheter, logguppgifter (exempelvis tidsstämplar, åtkomst) och liknande uppgifter.

För vårdtagare (notera att inte alla uppgifter är tillämpliga för alla vårdtagare);

namn och kontaktuppgifter, personnummer, andra typer av personrelaterade koder och person-ID, kön, medicinsk och hälsoinformation, betalningsinformation, tidsbokningar, födelseland, modersmål, familjesituation, släktband, anhöriga, samtyckesinformation, skola/skolklass och företagstillhörighet. Notera att möjligheter finns även till anteckningar som fritext i journalen och andra delar av systemet (i dessa fritextfält kan vilken typ av personuppgifter som helst antecknas, det är inte ovanligt att det här förekommer känsliga uppgifter av annan art än medicinska och hälsouppgifter).

Andra registrerade (se under rubriken Kategorier av registrerade ovan vilken typ av personer detta kan avse, notera att inte alla uppgifter är tillämpliga för alla vårdtagare);

namn och kontaktuppgifter, personnummer, yrkesroll, arbetsplats, koder kopplade till personen (exempelvis HSA-ID, förskrivarkod, laboratoriekod), relation till/händelser relaterade till/kontakter/diskussioner om/protokoll/minnesanteckningar med/avseende Vårdtagare och liknande uppgifter. Notera att möjligheter finns även till anteckningar som fritext i journalen och andra delar av systemet (i dessa fritextfält kan vilken typ av personuppgifter som helst antecknas, det är inte ovanligt att det här förekommer känsliga uppgifter av annan art än medicinska och hälsouppgifter).

Behandlingsaktiviteter

Nedan listade aktiviteter kan komma att genomföras av Personuppgiftsbiträdet inom ramen för behandlingen under Huvudavtalet.

Lagring, bearbetning eller ändring, insamling, registrering, strukturering, framtagning, läsning, användning, justering eller sammanförande, överföring, begränsning, radering eller förstöring, rättelser eller felsökning på uppdrag av Personuppgiftsansvarig utifrån vad som överenskommits med Personuppgiftsansvarig i Huvudavtalet samt enligt instruktioner till support/konsult/utvecklingsavdelning/drift eller annan personal hos Personuppgiftsbiträdet i specifika fall.

Plats för behandling av personuppgifterna

För samtliga kunder;

Behandling kan komma att genomföras av personal hos Personuppgiftsbiträdet vid bolagets kontor i Sverige i Uppsala, Stockholm och Göteborg, på plats hos Personuppgiftsansvarig om Personuppgiftsbiträdets personal bedriver support/installation på plats eller hos underbiträden som anges i Bilaga 2.

Fysisk lagring för kunder som har Personuppgiftsbiträdets hosting-tjänst i Sverige;

Datahall i Göteborgsområdet, Sverige.

Fysisk lagring för kunder som har Personuppgiftsbiträdets hosting-tjänst i Tyskland;

Datahall i Tyskland, Frankfurt.

Informationssäkerhet

Att skydda kunders informationstillgångar innehållande personuppgifter är en prioriterad fråga för Personuppgiftsbiträdet. Grundprinciper för Personuppgiftsbiträdets informationssäkerhet är; tillgänglighet, riktighet, konfidentialitet samt spårbarhet.

Bristande informationssäkerhet kan leda till störningar i kunders samhällsviktiga verksamhet och medföra risker för den personliga integriteten. Personuppgiftsbiträdet följer därför nedanstående riktlinjer för att säkerställda att ovanstående principer följs för all personuppgiftsbehandling:

- Identifiera, riskhantera och tilldela ansvar för informationstillgångar som innehåller personuppgifter samt vidta relevanta och balanserade skyddsåtgärder för dessa.
- Hantera informationstillgångar i enlighet med lagstiftning, policyer, riktlinjer samt kunders instruktioner.
- Utbilda och informera medarbetare i informationssäkerhet så att en god utbildningsnivå erhålls och bibehålls samt att informationssäkerheten tillämpas.
- Utforma och underhålla rutiner och verktyg för uppföljning som säkerställer informationssäkerheten.
- Utforma och underhålla rutiner och verktyg för incidenthantering för incidenter som rör personuppgiftsbehandling.
- Styra medarbetares tillgång till information, dvs. rätt information vid rätt tidpunkt och på rätt plats till en behörig användare.