



Sophiahemmet Rehab Center

PERSONUPPGIFTSPOLICY

Klient, leverantör & kund

Innehåll

PERSONUPPGIFTSPOLICY	1
1 INLEDNING OCH SYFTE	1
2 DEFINITIONER	2
2.1 Personuppgifter.....	2
2.2 Känsliga personuppgifter	2
2.3 Personuppgiftsansvarig	2
2.4 Personuppgiftsbiträde	2
2.5 Registrerad.....	3
2.6 Behandling	3
3 ÄNDAMÅLET MED PERSONUPPGIFTSBEHANDLINGEN	3
3.1 Allmänt	3
3.2 Patienter	4
3.3 Kunder	5
3.4 Leverantörer	7
3.5 SRC som personuppgiftsbiträde och personuppgiftsansvarig	8
4 RÄTTIGHETER.....	8
4.1 Rätt till tillgång	8
4.2 Rätt till rättelse, radering eller begränsning	9
4.3 Rätt till dataportabilitet	9
4.4 Rätt att återkalla samtycke	10
5 KONTAKTUPPGIFTER	10
6 ÄNDRINGAR AV POLICYN.....	10



Sophiahemmet Rehab Center

PERSONUPPGIFTSPOLICY

1 INLEDNING OCH SYFTE

Denna policy reglerar Sophiahemmet Rehab Centers (SRC) behandling av personuppgifter som personuppgiftsansvarig, och anger de krav om skydd och säkerställande av ändamålsenlig personuppgiftsbehandling som gäller i den personuppgiftsansvariges verksamhet. Policyn anger vilka grundläggande principer som ska gälla för behandling av registrerades personuppgifter i SRCs verksamhet, processer och system. SRC behandlar personuppgifter både i egenskap av personuppgiftsansvarig samt i egenskap av personuppgiftsbiträde.

Syftet med dessa regler är att säkerställa att SRC har ett lämpligt säkerhetsskydd för de personuppgifter som hanteras samt att den personliga integriteten beaktas i verksamheten.

Policyn avser sådan personuppgiftsbehandling som följer av Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (allmän dataskyddsförordning/General Data Protection Regulation, (GDPR)). SRC ska därutöver beakta sådan annan lag så som Patientdatalagen (2000:355), förordningar samt Socialstyrelsens föreskrifter och allmänna råd (HSLF-FS, SOSFS) som äger tillämpning på personuppgifter.

SRC arbetar med hälso- och rehabiliteringsinriktade tjänster för individ-, grupp- och organisationer. Syftet med verksamheten är att ge förutsättningar för hållbar hälsa och god arbetsmiljö. SRC levererar tjänsterna utifrån egen verksamhet i Stockholm och Göteborg och genom underleverantörer över stora delar av Sverige. Inom verksamheten behandlas personuppgifter, varav vissa uppgifter är känsliga.

SRC respekterar och värnar om personlig integritet och ser till att personuppgifterna behandlas med betydande trygghet. Denna personuppgiftspolicy (Policyn) innehåller regler och riktlinjer för den behandling av personuppgifter som görs av SRC i egenskap av personuppgiftsansvarig samt personuppgiftsbiträde. Policyn är riktad såväl till anställda, patienter, kunder, leverantörer och samarbetspartners.

SRC har utsett dataskyddsombud som övervakar verksamhetens efterlevnad av dataskyddsförordningen och andra lagar, förordningar och föreskrifter som gäller för behandling av personuppgifter. Kontaktuppgifter längst ner i detta dokument.



Sophiahemmet Rehab Center

2 DEFINITIONER

Samtliga definitioner nedan ska ha den betydelse som följer av Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (allmän dataskyddsförordning).

2.1 Personuppgifter

Varje upplysning som avser en identifierad eller identifierbar fysisk person, varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringssuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

2.2 Känsliga personuppgifter

Med känsliga personuppgifter avses till exempel uppgifter om medlemskap i en fackförening och uppgifter om hälsa och uppgifter om en fysisk persons sexualliv eller sexuella läggning, genetiska uppgifter och biometriska uppgifter som entydigt identifierar en person.

2.3 Personuppgiftsansvarig

Det bolag som bestämmer ändamålen och medlen för behandlingen av personuppgifter.

2.4 Personuppgiftsbiträde

En fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar person-uppgifter för Skandias räkning.



Sophiahemmet Rehab Center

2.5 Registrerad

En registrerad är den fysiska person vars personuppgifter behandlas av SRC. För SRCs räkning är detta normalt en patient, försäkrad, leverantör, anställd, konsult eller samarbetspartner som är fysisk person. Det kan också röra sig om fysiska personer som inte är kunder i SRC, men som har en anknytning till någon av de nämnda fysiska personerna t ex gode män.

2.6 Behandling

En åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.

3 ÄNDAMÅLET MED PERSONUPPGIFTSBEHANDLINGEN

3.1 Allmänt

På SRC gäller sekretess och tystnadsplikt generellt på verksamheten. SRC begär in personuppgifter för att:

- uppfylla lagstadgade krav som uppställs för en bra och säker vård
- upprätta avtal med kunder och leverantörer
- administrera ekonomi, påminnelser, enkäter och statistikuppföljning som syftar till utvärderingar och kvalitetsutveckling

Nedan följer en mer ingående beskrivning.



Sophiahemmet Rehab Center

3.2 Patienter

För att patienter ska få en god och säker vård hos SRC behöver vi som vårdgivare inhämta personuppgifter. Dessa personuppgifter registreras i det vårdregister SRC använder. Vi behandlar personuppgifter inom hälso- och sjukvården för:

- patientjournalen och annan dokumentation som behövs för din vård
- administration i syfte att ge rätt vård
- annan dokumentation som följer av lag, förordning eller annan författning
- utveckling och kvalitetssäkring av vården
- planering, utvärdering och verksamhetsuppföljning
- upprättande av statistik

Behandlingen av personuppgifter för uppfyllande av dessa ändamål är reglerad i patientdatalagen (2008:355). Vissa personuppgifter kan också behandlas på grund av att SRC har en rättslig skyldighet till det. Exempelvis kan det röra sig om personuppgifter på fakturor/fakturabilagor till följd av bokföringsskyldighet.

Vid varje behandling av känsliga uppgifter vidtar SRC alltid lämpliga säkerhetsåtgärder för att skydda uppgifterna. Exempel på säkerhetsåtgärder som vidtas är behörighetsbegränsning för åtkomst till patientuppgifter och interna loggkontroller.

För vissa personuppgiftsbehandlingar behöver vi samtycke, t ex för att få göra digitala utskick via e-post eller sms för påminnelser om bokad tid eller exempelvis för fullmakt att inhämta journaluppgifter från andra vårdgivare eller handlingar från myndigheter.

Vi samlar bara in personuppgifter som är nödvändiga för att uppfylla ändamålen med personuppgiftsbehandlingen såsom:

- namn
- personnummer
- adress
- kontaktuppgifter
- e-postadress
- hälsorelaterade uppgifter

I regel bevaras patientjournaler och de personuppgifter som finns där i minst 10 år från senaste vårdtillfället. Patientprofiler som läggs upp i de digitala plattformar som SRC använder för säker och lagenlig kommunikation sparas i högst 1,5 år. Tillhörande



Sophiahemmet Rehab Center

patientdata, d.v.s. kontaktuppgifter etc., sparas i 7 dagar. Uppgifter för patient- och ekonomiadministration bevaras så länge som laglig grund för behandlingen föreligger och det anses nödvändiga att bevara dessa uppgifter. Efter det kommer de att raderas eller avidentifieras så att de inte längre går att koppla till en person.

3.3 Kunder

För att kunna ingå och hantera avtal med våra kunder behandlar SRC personuppgifter tillhörande personer som är företrädare för kunder. Vissa personuppgifter kan också behandlas på grund av att SRC har en rättslig skyldighet till det, exempelvis personuppgifter på vissa fakturor till följd av bokföringsskyldighet.

Vi behandlar personuppgifter avseende företrädare på bolag som vi har kundavtal med direkt eller via Skandias Hälsokedja eller som är potentiella kunder.

Personuppgifter som behandlas är:

- befattning
- namn
- telefonnummer
- e-postadress

De som behandlar uppgifterna är huvudsakligen för avtalet relevanta personer på SRC såsom:

- kundsamordnare
- kundansvariga
- ekonomiavdelningen
- anställda hos SRC som utför hälso-, rehabiliterings- och arbetsmiljötjänsterna
- underleverantörer till SRC
- underleverantörer inom Skandias Hälsokedja

För de fall när det finns ett befintligt kundavtal behandlar SRC enbart personuppgifter som är relevanta för kundförhållandet och som krävs för fullgörandet av avtalet. Personuppgifter så som företrädarens befattning, namn, e-post och telefonnummer behandlas för att kunna föra dialog med kunden och kunna administrera kundavtalet.



Sophiahemmet Rehab Center

Företrädares personuppgifter kan även behandlas för ändamålet att skicka intressanta erbjudanden till kundbolaget. För de fall SRC behandlar personuppgifter avseende företrädare för potentiella kunder, görs detta i syfte att ta kontakt med kunden för att kunna ge kunden information via telefon, e-post eller för att administrera möten. Företrädaren har dock rätt att när som helst invända mot behandling av personuppgifter för direktmarknadsföring vilket beskrivs närmare nedan under punkten 3.2.

Personuppgifter såsom medarbetares namn, personnummer och e-post behandlas vid planering av tjänsteleveranser och vid själva tjänsteleveransen vilken utförs av anställda hos SRC, underleverantörer till SRC eller underleverantörer till försäkringsaktiebolaget Skandia inom Skandias Hälsokedja. E-postadresser används vid inbjudningar till nyttjande av tjänst och vid utskick av enkäter som ingår som ett led i kvalitetsuppföljningen av de tjänster som erbjuds till kund. Enkätssammanställningarna görs på gruppnivå med säker aidentifiering. För företag med mindre antalet anställda görs inga

sammanställningar. Namn och personnummer används även som underlag för hantering av bokföring vilket främst rör kontroll av leverantörsfakturor samt fakturering till kund.

SRC lagrar aldrig uppgifter längre än nödvändigt med hänsyn till ändamålen med behandlingen. Vi genomför därför regelbundna gallringar bland lagrade personuppgifter och tar bort de uppgifter som inte längre behövs efter det att kundrelationen upphört.

SRC kan dock behöva lagra personuppgifterna efter det att kundrelationen upphört, bland annat för att kunna hantera eventuella rättsliga krav som kan tänkas riktas mot oss. Undantagsvis sparas därför personuppgifter viss tid efter grundförhållandets upphörande eller tills att personen invänt mot exempelvis direktmarknadsföring.

Personuppgifter avseende företrädare för potentiella kunder tas bort när dialogen med kunden upphört, under förutsättning att ingen kundrelation inletts, eller direkt om personen invänder mot direktmarknadsföring.

Tillgängligheten till sparade personuppgifter såsom medarbetares namn, personnummer och e-post är begränsad till kundansvariga samt ekonomiavdelningen/stab. Uppgifterna sparas under det år då tjänsten genomförs samt de två efterföljande åren, därefter gallras de bort. Sparandet under de tre åren görs för att kunna ge återkoppling till kund på vilka som genomgått tjänsten under tjänsteåret men även vid återkommande tjänst t ex hälsoundersökningar vart annat år vilket är vanligt förekommande.



Sophiahemmet Rehab Center

Personuppgifter kan också mer generellt behöva lagras för att säkerställa uppfyllelse av legala skyldigheter, exempelvis avseende bokföring. Om sådan skyldighet föreligger kan personuppgifterna sparas i minst 7 år.

3.4 Leverantörer

För att kunna ingå och hantera avtal med leverantörer behandlar SRC personuppgifter tillhörande personer som är företrädare för leverantörerna. Vissa personuppgifter kan också behandlas på grund av att SRC har en rättslig skyldighet till det, exempelvis personuppgifter på fakturor till följd av bokföringsskyldighet.

Vi behandlar personuppgifter avseende företrädare på företag som levererar tjänster och varor som vi har eller avser att ingå avtal med. Personuppgifter som behandlas kan bland annat vara:

- namn
- telefonnummer
- e-postadress
- adress
- yrkestitel.

De som mottar uppgifterna är huvudsakligen SRCs VD, enhetschefer, leverantörssamordnare, ekonomiavdelningen och administration.

SRC behandlar personuppgifterna för att generellt kunna administrera samarbetsavtal och inköpsavtal, hantera fakturor och för att kunna ställa de frågor som är relevanta avseende de varor eller tjänster som köps in från underleverantörerna. SRC behandlar även personuppgifter för att kunna förmedla uppdrag till underleverantörerna.

Sophiahemmet Rehab Center lagrar aldrig uppgifter längre än nödvändigt med hänsyn till ändamålen med behandlingen. SRC genomför därför regelbundna gallringar bland lagrade personuppgifter och tar bort de uppgifter som inte längre behövs efter det att avtalsrelationen upphört. SRC kan dock behöva lagra personuppgifterna efter det att avtalsrelationen upphört, bland annat för att administrera eventuella garantier och reklamationsfrister samt för att hantera rättsliga krav som kan tänkas riktas mot oss. Undantagsvis sparas därför personuppgifter i 2 år från avtalsförhållandets upphörande. Personuppgifter kan också mer generellt behöva lagras för att säkerställa uppfyllelse av legala skyldigheter, exempelvis avseende bokföring. Om sådan skyldighet föreligger kan personuppgifterna sparas i minst 7 år.



Sophiahemmet Rehab Center

3.5 SRC som personuppgiftsbiträde och personuppgiftsansvarig

SRC behandlar personuppgifter antingen genom att själva samla in dessa eller på uppdrag av externa parter. SRC kan därmed agera både som personuppgiftsansvarig och som personuppgiftsbiträde. I vissa fall kan vi även ha ett gemensamt personuppgiftsansvar med en annan extern aktör.

I de fall SRC behöver överlämna information till relevant tredje part (inklusive, men inte begränsat till situationer där vi har en rättslig skyldighet till det) har SRC som rutin att upprätta biträdesavtal för att behandlingen av personuppgifter ska ske på ett tryggt och säkert sätt. I biträdesavtalen anges alltid föremålet för behandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter och kategorier av registrerade samt våra skyldigheter och rättigheter som personuppgiftsansvariga. SRC ger även instruktioner till personuppgiftsbiträdet som personuppgiftsbiträdet är skyldig att följa.

SRC ingår alltid personuppgiftsbiträdesavtal med personuppgiftsansvarig i de fall bolaget agerar som personuppgiftsbiträde. Det är i dessa fall personuppgiftsansvarig som bestämmer exempelvis ändamål och lagringstider för personuppgifterna. När SRC är personuppgiftsbiträde behandlas alltså personuppgifterna i enlighet med personuppgiftsbiträdesavtalet och i enlighet med personuppgiftsansvariges instruktioner.

4 RÄTTIGHETER

4.1 Rätt till tillgång

Den fysiska person som är registrerad hos SRC har rätt att begära tillgång till de personuppgifter som vi behandlar och även informeras om bland annat ändamålen med behandlingen och vilka som mottagit personuppgifterna. SRC ska i egenskap av personuppgiftsansvarig förse den registrerade med kostnadsfri kopia på de personuppgifter som behandlas. Vid eventuella extra kopior kan SRC komma att ta ut en administrationsavgift.

Vad gäller patientjournaler får SRC bara lämna ut uppgifter om varken patienten eller någon närstående till patienten lider men av ett utlämnande. Utgångspunkten är att utlämnandet ska ske med patientens samtycke. I vissa situationer har SRC dock enligt lagstiftning uppgiftsskyldighet gentemot landsting och myndigheter. För journaler gäller



Sophiahemmet Rehab Center

sekretess och tystnadsplikt. Obehöriga hindras från att få tillgång till personuppgifter och känsliga personuppgifter genom olika säkerhetsåtgärder.

4.2 Rätt till rättelse, radering eller begränsning

Den fysiska person som är registrerad hos SRC har rätt att utan onödigt dröjsmål få sina personuppgifter rättade eller, under vissa förutsättningar, begränsade eller raderade. Om den fysiska personen anser att SRC behandlar personuppgifter som är felaktiga eller ofullständiga kan denne kräva att få dessa rättade eller kompletterade. Det finns även en rättighet att få uppgifter raderade om de inte längre är nödvändiga eller om behandlingen baseras på samtycke och detta har återkallats.

Företrädare för leverantörer och kunder har även rätt att när som helst invända mot behandling av dennes personuppgifter om dessa behandlas för direkt marknadsföring.

För patientjournaler gäller särskilda regler enligt patientdatalagen, föreskrifter och allmänna råd (HSLF-FS, SOSFS). Anteckningar som gjorts i en journal anses enligt lag vara låsta och därför kan dessa inte ändras eller raderas. Om en patient anser att en uppgift är felaktig kan vårdgivaren införa en rättelse i journalen. En rättelse är en notering som hänvisar till den felaktiga uppgiften. Både den ursprungliga anteckningen och rättelsen ligger därmed kvar i patientjournalen. Detta under förutsättning att patienten och vårdgivaren är överens om att anteckningen skall rättas. Är vårdgivaren och patienten oense kan en ansökan till tillsynsmyndigheten Inspektionen för vård och omsorg, IVO göras. Efter prövning av IVO rättas eller raderas journalen i enlighet med myndighetens beslut.

4.3 Rätt till dataportabilitet

Kunder och leverantörer har rätt till att få ut de personuppgifter som dessa har tillhandahållit den personuppgiftsansvarige och har rätt att överföra dessa uppgifter till en annan personuppgiftsansvarig. Detta gäller dock under förutsättning att det är tekniskt möjligt och den lagliga grunden för behandlingen utgörs av samtycke eller att behandlingen varit nödvändig för fullgörande av avtal. Dataportabiliteten omfattar inte patientdatajournaler.



Sophiahemmet Rehab Center

4.4 Rätt att återkalla samtycke

Om personuppgiftsbehandlingen grundar sig på ditt samtycke har du alltid rätt att återkalla detta samtycke, varpå personuppgiftsbehandlingen upphör att gälla. Sådan återkallelse påverkar dock inte lagligheten i behandlingen av personuppgifter som gjorts innan samtycket återkallades.

5 KONTAKTUPPGIFTER

Vid frågor om Policyn eller vid andra önskemål avseende personuppgifter, vänligen kontakta Sophiahemmet Rehab Centers dataskyddsombud Andrea Hemming på andrea.hemming@imrab.se

6 ÄNDRINGAR AV POLICYN

SRC förbehåller sig rätten att ändra och uppdatera Policyn. Vid materiella ändringar i Policyn eller om befintlig information ska behandlas på annat sätt än vad som anges i Policyn, kommer SRC att informera om detta på lämpligt sätt.