Riktlinje för behandling av personuppgifter vid Karolinska Universitetssjukhuset

Karolinska Universitetssjukhuset behandlar dagligen en stor mängd personuppgifter i samband med vård, administration, kvalitetsarbete, forskning m.m. Sjukhuset värnar om den personliga integriteten hos de personer vars uppgifter behandlas i verksamheten och det är viktigt att hanteringen sker på ett sätt som är förenligt med såväl tillämplig lagstiftning som sjukhusets interna riktlinjer.

I denna riktlinje beskrivs på ett övergripande sätt innehållet och tillämpningen av *dataskyddsförordning (GDPR) och kompletterande nationell lagstiftning* vid behandling av personuppgifter vid Karolinska Universitetssjukhuset verksamhet.

Dataskyddsförordningen och kompletterande nationell lagstiftning

Dataskyddsförordningen gäller vid all behandling av personuppgifter. Förordningen anger ramarna för när och under vilka omständigheter personuppgiftsbehandling är tillåten. Utöver dataskyddsförordningen ska kompletterande regler i svensk lagstiftning tillämpas vid behandling av personuppgifter, däribland patientdatalagen (2008:355) och Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården (HSLF-FS 2016:40).

Regelverket kring sekretess återfinns alltjämt huvudsakligen i offentlighets- och sekretesslagen (2009:400).

Roller och ansvar

Personuppgiftsansvarig

Karolinska Universitetssjukhuset är som organisation vanligtvis ***personuppgiftsansvarig*** för den behandling av personuppgifter som sker inom ramen för sjukhusets verksamhet. Sjukhusets styrelse är ytterst ansvarig för att sjukhusets behandling av personuppgifter sker i enlighet med dataskyddsförordningens föreskrifter.

Personuppgiftsbiträde

I de fall Karolinska Universitetssjukhuset behandlar personuppgifter för annans räkning, är sjukhuset ***personuppgiftsbiträde***.

Medarbetare

Varje enskild ***medarbetare*** ansvarar för att följa gällande regelverk och riktlinjer inom ramen för

den personuppgiftsbehandling som den enskilde medarbetaren utför.

Dataskyddsombud
Karolinska Universitetssjukhuset har ***dataskyddsombud,*** vilkas roll är att övervaka att dataskyddsförordningen och kompletterande lagstiftning följs på sjukhuset, genom att till exempel utföra kontroller och ge information och råd inom organisationen. Dataskyddsombuden har ett nära samarbete med sjukhusets informationssäkerhetssamordnare.

Informationssäkerhetssamordnare
Karolinska Universitetssjukhuset har en ***informationssäkerhetssamordnare*** som ska ansvara för informationssäkerhetsarbetet inom organisationen. Samordnaren har ett nära samarbete med sjukhusets dataskyddsombud.

Informationssäkerhetskoordinator
Varje tema, funktion och stab har en utsedd ***informationssäkerhetskoordinator***. Koordinatorns ansvar är att tillsammans med informationssäkerhetssamordnaren och dataskyddsombuden koordinera arbetet kring data- och integritetskyddsfrågor inom respektive verksamhet.

Definitioner

Dataskyddsförordningen gäller vid behandling av personuppgifter.

Personuppgift	Varje upplysning som avser en identifierad eller en identifierbar fysisk person. Det kan till exempel vara namn, personnummer, kundnummer, ljudupptagningar, foton, krypterad information och elektroniska identiteter (t ex IP-adresser). *Vid hantering av data som är avidentifierad/anonymiserad gäller inte dataskyddsförordningen. ”Avidentifierad/anonymiserad” innebär att uppgifterna inte på något sätt går att härleda till en fysisk person. Att uppgifter är ”pseudonymiserade”, exempelvis att man har ersatt namn och personnummer med ett kodnummer eller motsvarande, innebär inte att de är avidentifierade/anonymiserade. Uppgifter som är pseudonymiserade utgör därför personuppgifter.*
Identifierbar fysisk person	En person som direkt eller indirekt kan identifieras särskilt med hänvisning till namn, ett identifikationsnummer, en lokaliseringsuppgift eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet. Dataskyddsförordningen gäller inte vid behandling av

	personuppgifter rörande avlidna personer.
Personuppgiftsbehandling	En åtgärd eller en kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej. Exempelvis 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.

Principer för behandling av personuppgifter

Vid **all** behandling av personuppgifter inom sjukhuset ska följande principer följas:

- **Laglighet, korrekthet och öppenhet**
  Uppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade, dvs. den person vars personuppgifter behandlas.

  Sjukhuset får endast behandla personuppgifter om det finns en **rättslig grund** och under förutsättning att gällande lagstiftning följs. Den registrerade (dvs. den vars personuppgifter behandlas) ska ges möjlighet till insyn i behandlingen och uppgifter ska alltid behandlas med stor hänsyn till den enskildes integritet.

- **Ändamålsbegränsning**
  Uppgifterna ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål. Den som behandlar personuppgifter vid sjukhuset måste vara medveten om och tydligt dokumentera ändamålet med behandlingen och ansvarar också för att personuppgifterna inte behandlas för andra ändamål än det ursprungliga ändamålet.

- **Uppgiftsminimering**
  Uppgifterna ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas.

  Sjukhuset ska endast använda sig av de personuppgifter som krävs för att uppnå ändamålet med personuppgiftsbehandlingen. Personuppgiftsbehandlingen får inte bli mer omfattande än vad som krävs i förhållande till det ändamål för vilket de behandlas. Denna princip är extra viktig när det rör sig om behandling av känsliga personuppgifter (t.ex. uppgifter om hälsa).

- **Riktighet**
  Uppgifterna ska vara riktiga och om nödvändigt uppdaterade. Alla rimliga åtgärder ska vidtas för att säkerställa att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas raderas eller rättas utan dröjsmål.

  Sjukhuset ska alltid verka för att personuppgifter som är felaktiga rättas och måste ha tydliga rutiner för hur felaktiga uppgifter ska behandlas.

- **Lagringsminimering**
  Uppgifterna får inte förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändig för de ändamål för vilka personuppgifterna behandlas.

  När ändamålet är uppnått eller inte längre aktuellt ska uppgifterna behandlas utifrån gällande regler om bevarande och gallring.

- **Integritet och konfidentialitet**
  Uppgifterna ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder.

  Personuppgifter ska skyddas genom lämpliga tekniska och organisatoriska åtgärder. Uppgifternas beskaffenhet (känslighet) och riskerna med behandlingen blir avgörande i bedömningen av vilka skyddsåtgärder som är aktuella. Det måste göras en bedömning av varje enskild personuppgiftsbehandling. Vägledning finns i sjukhusets riktlinje om informationssäkerhet.

- **Ansvarsskyldighet**
  Karolinska Universitetssjukhuset ansvarar för att kunna *visa* att samtliga ovanstående principer följs vid sjukhuset. Sjukhuset ska därför dokumentera samtliga personuppgiftsbehandlingar och vilka åtgärder som vidtas för att kontrollera efterlevnad.

Rättslig grund vid behandling av personuppgifter

För att Karolinska Universitetssjukhuset ska få behandla personuppgifter måste det finnas en **rättslig grund** för behandlingen. Inom hälso- och sjukvården får personuppgifter behandlas för olika ändamål och den rättsliga grunden varierar beroende på för vilket ändamål uppgifterna behandlas.

Stora delar av de uppgifter som behandlas vid sjukhuset är **känsliga personuppgifter** (i dataskyddsförordningen går dessa under benämningen ”särskilda kategorier av personuppgifter”). Hit hör personuppgifter som avslöjar *ras* eller *etniskt ursprung*, *politiska åsikter*, *religiös eller filosofisk övertygelse* eller *medlemskap i fackförening* samt *genetiska uppgifter*, *biometriska uppgifter för att entydigt identifiera en fysisk person*, *uppgifter om hälsa* eller *uppgifter om en fysisk persons sexualliv eller sexuella läggning*.

För behandling av känsliga personuppgifter krävs, **utöver** en rättslig grund för behandlingen av personuppgifter som sådan, även stöd i något av undantagen (s.k. ytterligare rättslig grund) som medger behandling av just känsliga personuppgifter. Känsliga personuppgifter ska alltid ges ett högt skydd mot obehörig åtkomst.

Rättsliga grunder för behandling av **personuppgifter** vid sjukhuset kan vara:

Samtycke	Den registrerade har lämnat sitt uttryckliga samtycke till personuppgiftsbehandlingen. *Samtycket måste vara frivilligt och specifikt formulerat. Den som samtycker måste ha försetts med klar, tydlig och lättbegriplig information om vad denne samtycker till. Samtycket får inte innehålla några oskäliga villkor. Den som behandlar personuppgifter med stöd av den registrerades samtycke måste kunna visa att samtycket har lämnats.* *Kravet på frivillighet gör att det i många fall inte är tillåtet eller lämpligt att använda samtycke som rättslig grund för behandling av personuppgifter när ett ojämlikt maktförhållande råder mellan den som vill utföra en behandling av personuppgifter, och den vars personuppgifter ska registreras. Detta utesluter ofta användning av samtycke som rättslig grund i relationen mellan vårdgivare och patient, och i relationen mellan arbetsgivare och anställda. Det bör alltid övervägas om det går att stödja personuppgiftsbehandlingen på någon av de andra rättsliga grunderna.* *Observera att ovanstående begränsning avseende samtycke som rättslig grund gäller utifrån dataskyddsförordningen. Det kan alltjämt vara nödvändigt att inhämta samtycke enligt annan lagstiftning, t.ex. enligt etikprövningslagen i samband med forskning.* *Om den rättsliga grunden för en behandling av personuppgifter är att det har inhämtats ett samtycke från den registrerade så har denne rätt att när som helst återkalla samtycket. Ett återkallande av samtycket påverkar dock inte lagligheten av personuppgiftsbehandlingen för*

	tiden innan samtycket återkallades. *(För mer information om samtycke, se art. 7 dataskyddsförordningen)*
Avtal	Den registrerade har ingått eller ska ingå ett avtal med sjukhuset. *För att ett avtal med den registrerade ska kunna användas som rättslig grund krävs att behandlingen av personuppgifterna är nödvändig antingen för att fullgöra avtalet med den registrerade eller för att vidta åtgärder på begäran av den registrerade innan avtalet ingås.*
Rättslig förpliktelse	Det finns lagar eller regler som gör att sjukhuset måste behandla vissa personuppgifter i sin verksamhet.
Myndighetsutövning och uppgift av allmänt intresse	Sjukhuset måste behandla personuppgifter för att utföra sina myndighetsuppgifter eller för att utföra en uppgift av allmänt intresse.
Grundläggande intresse	Sjukhuset måste behandla personuppgifter för att skydda en registrerad som inte kan lämna samtycke, t.ex. om den är medvetslös.

Undantag (s.k. ytterligare rättslig grund) som medger behandling av **känsliga personuppgifter** vid sjukhuset:

Samtycke	Den registrerade har uttryckligen lämnat sitt samtycke till behandling av känsliga personuppgifter för ett eller flera specifika ändamål.
För att skydda någons grundläggande intressen	Om den registrerade är fysiskt eller rättsligt förhindrad att ge sitt samtycke och behandlingen är nödvändig för att skydda den registrerade eller någon annan fysisk persons grundläggande intressen, t.ex. om en person har blivit plötsligt sjuk och förlorat medvetandet.
När någon själv har offentliggjort de känsliga uppgifterna	Om någon på eget initiativ på ett tydligt sätt har offentliggjort känsliga uppgifter om sig själv får andra också behandla de uppgifterna, t.ex. om personen ifråga framträder i tv och berättar om sin sjukdom. *Det är personens avsikt som avgör om man kan säga att den själv har offentliggjort uppgifterna. Den som bara deltar i ett möte som*

	anordnats av en fackförening har troligen inte haft som avsikt att berätta offentligt att den är medlem i fackföreningen. Samma sak gäller för uppgifter som förekommer i en rättegång i domstol.
För att fullgöra skyldigheter inom arbetsrätt, social trygghet och socialt skydd	Behandlingen är nödvändig för att sjukhuset ska kunna fullgöra sina skyldigheter och utöva sina särskilda rättigheter i egenskap av arbetsgivare, t.ex. vid utbetalning av sjuklön och genomförande av rehabilitering. Denna rättsliga grund förutsätter att behandlingen är tillåten enligt svensk rätt eller kollektivavtal.
Viktigt allmänt intresse	Om det är nödvändigt av hänsyn till ett viktigt allmänt intresse är det tillåtet att behandla känsliga personuppgifter. Detta kan vara fallet när en myndighet tar emot personuppgifter och enligt lag måste behandla dem, om behandlingen är nödvändig för att myndigheten ska kunna handlägga ett ärende eller om behandlingen är nödvändig med hänsyn till viktigt allmänt intresse. Ett exempel på ett viktigt allmänt intresse är den grundlagsfästa rätten att ta del av allmänna handlingar.
Hälso- och sjukvård och social omsorg.	Behandlingen är nödvändig inom hälso- och sjukvård och social omsorg. Detta förutsätter att behandlingen har stöd i svensk lag, t.ex. i patientdatalagen eller biobankslagen, och att uppgifterna behandlas av eller under ansvar av en yrkesutövare som omfattas av (lagstadgad) tystnadsplikt.
Arkivändamål, forskningsändamål eller statistiska ändamål.	Behandlingen är nödvändig för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål (kräver godkänd etikprövning) eller statistiska ändamål.

Den rättsliga grunden, samt tillämpligt undantag vid behandling av känsliga personuppgifter, ska alltid dokumenteras. Sjukhuset ska också alltid informera de registrerade med vilken rättslig grund vi behandlar dennes personuppgifter.

Personnummer och samordningsnummer

Ett personnummer anses vara en extra skyddsvärd personuppgift. Huvudregeln är att den registrerades samtycke måste inhämtas för att få behandla personnummer. Om det inte finns samtycke är behandling av personnummer tillåtet om det är klart motiverat med hänsyn till:

- ändamålet med behandlingen,
- vikten av en säker identifiering, eller
- något annat beaktansvärt skäl

Personnummer och samordningsnummer bör exponeras i så liten omfattning som möjligt.

Information till den registrerade

Den registrerade har rätt att få koncis, tydlig och lättbegriplig information när hans eller hennes personuppgifter behandlas.

Information om personuppgiftsbehandlingen ska lämnas av den personuppgiftsansvarige både när uppgifterna samlas in och när den registrerade annars begär det.

Om personuppgifter som rör en registrerad person samlas in från den registrerade (t.ex. vid deltagande i forskning, kliniska studier, nationella kvalitetsregister m.m.), ska den personuppgiftsansvarige, när personuppgifterna erhålls, till den registrerade lämna information om följande:

- Identitet och kontaktuppgifter för den personuppgiftsansvarige (dvs. Karolinska Universitetssjukhuset) och dess företrädare, dvs. den/de som i praktiken ansvarar för den aktuella personuppgiftshanteringen.

- Kontaktuppgifter till dataskyddsombudet:

  Dataskyddsombudet, Karolinska Universitetssjukhuset, 171 76 Solna, tel: 08-517 700 00 (växel), e-post: dataskyddsombud.karolinska@regionstockholm.se

- De kategorier av personuppgifter som behandlingen gäller, utifall uppgifterna inte samlas in direkt från den registrerade.

- Ändamålen med personuppgiftsbehandlingen samt rättslig grund.

- Eventuella mottagare av personuppgifterna. I den utsträckning det är möjligt ska mottagarna namnges, annars kan kategorierna av mottagare anges så specifikt som möjligt.

- I tillämpliga fall: Att den personuppgiftsansvarige avser att överföra personuppgifter till ett tredjeland (dvs. ett land utanför EU/EES) eller en internationell organisation samt vilka skyddsåtgärder som kommer att vidtas i anslutning till sådan behandling. I den

utsträckning det är möjligt ska anges vilket/vilka länder utanför EU/EES som uppgifterna överförs till.

- Den tidsperiod under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period.

- Att det föreligger en rätt att av den personuppgiftsansvarige begära registerutdrag, rättelse eller radering av personuppgifter eller begränsning av behandling som rör den registrerade eller att invända mot behandling samt rätten till dataportabilitet.

- Om personuppgiftsbehandlingen grundar sig på samtycke: Att det föreligger en rätt att när som helst återkalla sitt samtycke, utan att detta påverkar lagligheten av behandlingen på grundval av samtycket, innan detta återkallades.

- Rätten att lämna in klagomål till Integritetsskyddsmyndigheten.

- Om insamlingen av uppgifterna är ett lagkrav eller ett krav enligt avtal.

Om den personuppgiftsansvarige avser att ytterligare behandla personuppgifterna för ett annat syfte än för vilket de insamlades, ska den personuppgiftsansvarige, före denna ytterligare behandling, ge den registrerade information om detta andra syfte samt ytterligare relevant information enligt förteckningen ovan.

(För mer information om vilken information som ska lämnas till registrerade, se art. 13 och 14 i dataskyddsförordningen)

Den registrerades rättigheter

- **Information**
  Den registrerade har rätt att få information i enlighet med ovanstående avsnitt.

  Observera att det kan finnas skyldighet att lämna information även i annan lagstiftning, t.ex. i patientdatalagen. Detta kan göra att mer information måste lämnas än den som krävs enligt dataskyddsförordningen.

- **Registerutdrag**
  Den registrerade har rätt att få veta huruvida hans eller hennes personuppgifter behandlas vid sjukhuset. Om personuppgifterna behandlas har han eller hon rätt att få information om bl.a. ändamålen med behandlingen, kategorier av personuppgifter som behandlingen gäller och mottagare till vilka personuppgifterna har eller ska lämnas ut. Se sjukhusets

riktlinje om registerutdrag [STAB2682]. Registerutdrag hanteras av enheten Registratur och Informationshantering.

Patienter har också rätt att få information om vid vilken vårdenhet och vid vilken tidpunkt någon har haft åtkomst till en patients uppgifter (loggutdrag). Denna rättighet regleras dock i patientdatalagen.

- **Rättelse**
  Den registrerade ska ha rätt att av den personuppgiftsansvarige utan onödigt dröjsmål få felaktiga personuppgifter som rör honom eller henne rättade.

  Vid hantering av uppgifter i patientjournal (t.ex. rättelse, avvikande mening eller journalförstöring) gäller patientdatalagen. Se sjukhusets riktlinje om felaktiga journaluppgifter [STAB0670].

- **Radering (”rätten att bli bortglömd”)**
  Beroende på omständigheter i det enskilda fallet och på vilken rättslig grund som personuppgiftsbehandlingen görs kan den registrerade ha rätt till radering av sina personuppgifter. Rättigheten har mycket begränsad betydelse inom sjukhusets verksamhet eftersom merparten av sjukhusets personuppgiftsbehandlingar vilar på en rättslig grund där rätten till radering inte är tillämplig.

  Denna rättighet är inte tillämplig på personuppgiftsbehandling som sker för hälso- och sjukvårdsändamål.

- **Begränsning av behandling**
  Under vissa förutsättningar har den registrerade rätt att begära att behandlingen av personuppgifter begränsas. Detta gäller under den tid som andra invändningar bedöms. Begränsning innebär att Karolinska Universitetssjukhuset inte får göra något med personuppgifterna mer än fortsätta lagra dem.

  Denna rättighet är inte tillämplig på personuppgiftsbehandling som sker för hälso- och sjukvårdsändamål.

- **Klagomål till tillsynsmyndighet**
  En registrerad som anser att en personuppgiftsbehandling som avser henne eller honom strider mot dataskyddsförordningen har rätt att lämna in klagomål till Integritetsskyddsmyndigheten.

(Läs mer om detta i art. 77 dataskyddsförordningen)

- **Skadestånd**
  En person som har lidit skada på grund av att hans eller hennes personuppgifter har behandlats i strid med dataskyddsförordningen kan ha rätt till skadestånd av den eller de personuppgiftsansvariga som har medverkat vid behandlingen. Den enskilde kan begära skadestånd från den personuppgiftsansvarige eller personuppgiftsbiträdet eller väcka skadeståndstalan i domstol.

Personuppgiftsbiträden

Den som behandlar personuppgifter för den personuppgiftsansvariges räkning kallas för **personuppgiftsbiträde**. Ett personuppgiftsbiträde kan vara en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ.

Om Karolinska Universitetssjukhuset ingår ett avtal/samarbete med en extern aktör som innebär att den externa aktören behandlar personuppgifter för sjukhusets räkning så måste det upprättas ett personuppgiftsbiträdesavtal. Sjukhuset har en mall för personuppgiftsbiträdesavtal som ska användas när sjukhuset i egenskap av personuppgiftsansvarig använder sig av ett personuppgifts-biträde.

Verksamhetschefen är behörig att skriva under personuppgiftsbiträdesavtal för Karolinska Universitetssjukhusets räkning. Personuppgiftsbiträdesavtal ska diarieföras.

(Läs mer om personuppgiftsbiträden i art. 28 dataskyddsförordningen.)

Överföringar av personuppgifter till land utanför EU/EES

Personuppgifter får överföras till land utanför EU/EES endast under vissa i dataskyddsförordningen angivna förutsättningar. Dessa är primärt:

- om det finns ett beslut från EU-kommissionen om att landet ifråga säkerställer att personuppgifterna är tillräckligt skyddade, s.k. adekvat skyddsnivå, eller

- om det har vidtagits lämpliga skyddsåtgärder för den specifika överföringen. För sjukhusets del är det framförallt tecknande av s.k. standardavtalsklausuler med mottagaren av personuppgifterna som är aktuellt. Se Data Transfer Agreement for Processors och Data Transfer Agreement for Controllers för mallar.

I vissa särskilda fall kan det vara tillåtet att överföra personuppgifter till land utanför EU/EES trots att mottagarlandet saknar adekvat skyddsnivå eller att tillräckliga och lämpliga

skyddsåtgärder inte har varit möjligt att vidta. Förutsättningarna för att använda denna överföringsmekanism är strikt reglerade i artikel 49 dataskyddsförordningen och flera av de alternativ som listas i artikeln kan inte användas till stöd för överföringar som sker av offentliga myndigheter, inbegripet Karolinska Universitetssjukhuset.

När överföring får ske enligt artikel 49:

- den registrerade uttryckligen har samtyckt till det, efter att ha fått information om riskerna med överföringen,
- överföringen är nödvändig för att fullgöra ett avtal mellan sjukhuset och den registrerade eller för att, på den registrerades begäran, genomföra åtgärder inför ett sådant avtal
- överföringen är nödvändig för att ingå eller fullgöra ett avtal med någon annan än den registrerade, om det ligger i den registrerades intresse,
- överföringen är nödvändig av viktiga skäl som rör allmänintresset,
- överföringen är nödvändig för att fastställa, göra gällande eller försvara rättsliga anspråk,
- överföringen är nödvändig för att skydda den registrerades eller andra personers grundläggande intressen, när den registrerade är fysisk eller rättsligt förhindrad att lämna samtycke, eller
- överföringen, under vissa förutsättningar, görs från ett register som enligt nationell rätt eller EU-rätten är för allmänhetens information.

Register över behandling

Den personuppgiftsansvarige (Karolinska Universitetssjukhuset) ska föra ett skriftligt och elektroniskt register över all behandling av personuppgifter.

Samtliga personuppgiftsbehandlingar vid sjukhuset ska anmälas i Privacy Records, DraftIt.

(Läs användarmanual för registrering av personuppgiftsbehandling. Finns på Inuti > Rättskansliet > Sjukhus- och myndighetsjuridik > Personuppgiftsbehandling (GDPR))

Säkerhet i samband med personuppgiftsbehandlingen

De personuppgifter som behandlas vid Karolinska Universitetssjukhuset ska skyddas mot

obehörig åtkomst. Det finns särskilda krav på säkerhetsåtgärder som bl.a. innebär att bara den som har behov av att ta del av personuppgifter får ha tillgång till dem och att det ska kontrolleras att ingen obehörig tagit del av uppgifter. Vilka säkerhetsåtgärder som ska vidtas beror på personuppgiftsbehandlingens art, omfattning, sammanhang och ändamål. Ju känsligare personuppgifter, desto högre krav på säkerhet.

Den som behandlar personuppgifter måste vidta **lämpliga tekniska och organisatoriska åtgärder** för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken. Exempel på säkerhetsåtgärder är **pseudonymisering** och **kryptering** av personuppgifter.

Frågor om säkerhet i samband med personuppgiftsbehandlingen kan besvaras av sjukhusets informationssäkerhetssamordnare.

(Läs mer om säkerhet i samband med personuppgiftsbehandling i art. 32 dataskyddsförordningen)

Riskanalys och konsekvensbedömning (DPIA)

Inför varje ny personuppgiftsbehandling ska analyseras vilka risker personuppgiftsbehandlingen kan innebära och föreslå lämpliga säkerhetsåtgärder.

En konsekvensbedömning ska göras om en personuppgiftsbehandling, särskilt med användning av ny teknik och med beaktande av dess art, omfattning, sammanhang och ändamål, sannolikt leder till en hög risk för fysiska personers rättigheter och friheter. Här avses i första hand dataskydd och integritet.

En konsekvensbedömning kan avse en enda behandling av personuppgifter eller en serie liknande behandlingar (vad gäller art, omfattning, innehåll, ändamål och risker). En konsekvensbedömning kan också vara användbar för att bedöma data- och integritetsskyddet för en teknisk produkt, t.ex. maskinvara eller programvara.

Den dokumenterade konsekvensbedömningen bör innehålla följande:

- En beskrivning av personuppgiftsbehandlingen
- En bedömning av behovet av behandlingen och om den står i proportion till syftet.
- En bedömning av riskerna med personuppgiftsbehandlingen.
- En bedömning av vilka åtgärder som behöver vidtas för att behandlingen ska kunna ske på ett säkert och rättsenligt sätt.

Vid konsekvensbedömning ska sjukhusets mall för konsekvensbedömning (DPIA) användas, se bilaga 1.

Personuppgiftsincidenter

En **personuppgiftsincident** är en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats. (art. 4.12 dataskyddsförordningen)

Vid en personuppgiftsincident ska sjukhuset utan onödigt dröjsmål och, om så är möjligt, inte senare än **72 timmar** efter att ha fått vetskap om den, anmäla personuppgiftsincidenten till tillsynsmyndigheten (Integritetsskyddsmyndigheten) såvida det inte är osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter.

Om anmälan till tillsynsmyndigheten inte görs inom 72 timmar ska den åtföljas av en motivering till förseningen.

Mer information om personuppgiftsincidenter finns i sjukhusets rutin om hantering av personuppgiftsincidenter.

Versionshistorik

Version	Datum	Förändring och kommentar	Ansvarig
9	2022-02-01	Uppdatering av DPIA-mall av Helin Yaser, jurist.	Helena Sundén
8	2021-11-12	Tillägg av bilaga DPIA-mall och bilaga GDPR riskanalysmall av Helin Yasar, jurist.	Helena Sundén
7	2021-11-10	Uppdatering och revidering av hela dokumentet av Helin Yasar, jurist.	Helena Sundén
6	2020-09-07	Övergripande uppdatering och revidering av dokumentet	Camilla Nortoft
5	2019-09-13	Revidering av formalia	Diana Färje
4	2019-08-16	Övergripande uppdatering och revidering av hela dokumentet	Diana Färje
3	-	-	
2	2018-05-25	Uppdaterat formatering	Diana Färje
1	2018-05-16	Skapat	Diana Färje