Novartis Sverige AB
Box 1150
183 11 TÄBY

Tillsyn enligt personuppgiftslagen (1998:204)- två forskningsprojekt vid Novartis Sverige AB

Datainspektionens beslut

Datainspektionen konstaterar att Novartis Sverige AB fortsätter att behandla personuppgifter i den extra framtida studien i forskningsprojektet CPJMR0092105 även om samtycket återkallats. Datainspektionen förelägger Novartis Sverige AB att i enlighet med 12 § personuppgiftslagen (1998:204) inte behandla ytterligare personuppgifter om den registrerade återkallat samtycket.

Datainspektionen förelägger Novartis Sverige AB att justera informationen till patienterna enligt följande:

- Datainspektionen konstaterar att informationen om vem som är personuppgiftsansvarig för forskningsstudien CPJMR0092105 är missvisande och att det är otydligt vem som är personuppgiftsansvarig i studien CRAD001A2314. Enligt 25 § personuppgiftslagen ska informationen till registrerade omfatta uppgift om den personuppgiftsansvariges identitet. Datainspektionen förelägger Novartis Sverige AB att i patientinformationen tydliggöra personuppgiftsansvaret för de aktuella studierna.
- Barn mellan 12-17 år som är föremål för studien CRAD001A2314, ska ges fullständig information i enlighet med 25 § personuppgiftslagen vilket innebär att i den granskade informationen ska tilläggas uppgift om den personuppgiftsansvariges identitet, mottagarna av uppgifterna, rätten att ansöka om registerutdrag och rättelse.

Datainspektionen förutsätter att Novartis Sverige AB följer kraven på säkerhetsåtgärder i 31 § personuppgiftslagen om känsliga personuppgifter behandlas över öppet nät i någon av de granskade studierna.

Ärendet avslutas.

Bakgrund

Datainspektionen inledde tillsyn den 20 februari 2014 gentemot Novartis Sverige AB för granskning av forskningsprojekt i vilka känsliga personuppgifter behandlas med stöd av samtycke. Novartis Sverige AB ombads inkomma med en lista över pågående forskningsprojekt som behandlade denna kategori av personuppgifter.

Datainspektionen begärde därefter att Novartis Sverige AB skulle lämna en närmare redogörelse för följande forskningsprojekt:

- CPJMR0092105
- CRAD001A2314

Det primära syftet med studien CPJMR0092105 är att samla in långtidsdata av synundersökningar och funktioner hos patienter med mutation i RLBP1 genen för att öka kunskapen om sjukdomen. Sekundärt kommer studien värdera de olika undersökningsmetoderna över tid för att ge information om vilka mätningar som bäst kan användas vid en behandlingsstudie samt identifiera patienter som eventuellt kan inkluderas i framtida behandlingsstudier. I anslutning till den nyss nämnda huvudstudien finns en extra studie den s.k. ”Extra framtida forskning”. Syftet med den extra studien är att bättre förstå näthinnesjukdomar genom att studera gener och DNA. De som deltar i studien är mellan 8-70 år. Uppgifter i studien kan komma att skickas inom eller utanför EU/EES. Av studiesammanfattningen framgår att bearbetning av insamlad studiedata sker av Novartis i USA. Studien är granskad och godkänd av regionala etikprövningsnämnden i Umeå.

Syftet med studie CRAD001A2314 är att undersöka effekt och säkerhet av immunsuppression med Certican i kombination med Prograf i minskad dos samt utsättande av kortison efter 6 månader, vid njurtransplantation till barn och ungdomar mellan 1 och 17 år. Resultatet kommer att jämföras med barn

och ungdomar som får standardbehandling. Uppgifter i studien kan komma att lämnas ut till bland annat samarbetspartners och den koncern som Novartis Sverige AB tillhör inom och utanför den Europeiska Unionen (EU). Studien är granskad och godkänd av regionala etikprövningsnämnden i Stockholm.

Novartis Sverige AB har uppgett att uttryckligt samtycke från samtliga registrerade ska utgöra den lagliga grunden för behandlingen av känsliga personuppgifter i dessa forskningsprojekt.

Rättsregler

Personuppgiftslagen

Det är personuppgiftslagen som reglerar förutsättningarna för behandling av personuppgifter i forskningsverksamhet.

Personuppgiftsansvaret

Personuppgiftsansvarig är enligt 3 § personuppgiftslagen den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter, och personuppgiftsbiträde är den som behandlar personuppgifter för den personuppgiftsansvariges räkning.
Vem som bestämmer över ändamålen avgörs genom en bedömning av de faktiska omständigheterna i det enskilda fallet. Avgörande för denna bedömning är bland annat varför behandlingen utförs och vem som är initiativtagare till behandlingen. Att bestämma över medlen för behandlingen avser främst att bestämma över de tekniska och organisatoriska medlen för behandlingen, dvs. ”hur” behandlingen ska gå till, till exempel vilka personuppgifter som ska behandlas, vilka tredje män som ska få tillgång till de behandlade personuppgifter och när uppgifter ska raderas.

Olika avtalskonstruktioner där personuppgiftsansvaret preciseras kan beaktas vid bedömningen men det är de faktiska omständigheterna i det enskilda fallet som är avgörande, dvs. vem eller vilka som faktiskt har bestämt över behandlingen, se *Personuppgiftslagen – En kommentar*, Öman och Lindblom, 4 uppl. 2011, s 93-94.

Vidare får ett personuppgiftsbiträde endast behandla uppgifter i enlighet med instruktioner från den personuppgiftsansvarige, se 30 § 1 st personuppgiftslagen. Den personuppgiftsansvarige kan överlåta den faktiska behandlingen av personuppgifter, men personuppgiftsansvaret kan aldrig överlåtas. Det är alltid den personuppgiftsansvarige som ytterst svarar för att personuppgiftslagen följs och att de registrerade behandlas korrekt.

Ansvaret är straff- och skadeståndssanktionerat. Den personuppgiftsansvarige är skadeståndsskyldig gentemot den registrerade, även för åtgärder som en medhjälpare eller ett personuppgiftsbiträde har utfört.

Känsliga personuppgifter

Enligt personuppgiftslagen är känsliga personuppgifter sådana som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening samt personuppgifter som rör hälsa eller sexualliv. Enligt huvudregeln i personuppgiftslagen är det förbjudet att behandla känsliga personuppgifter men det finns undantag. Känsliga personuppgifter får behandlas för forskningsändamål, enligt 19 § personuppgiftslagen, om behandlingen godkänts enligt lagen (2003:460) om etikprövning av forskning som avser människor (etikprövningslagen). Efter en lagändring den 1 juni 2008 utvidgades etikprövningslagen så att all forskning som innefattar behandling av sådana personuppgifter som avses i 13 och 21 §§ personuppgiftslagen ska etikprövas, oavsett om forskningspersonen lämnat sitt uttryckliga samtycke till behandlingen eller inte.

Vid etikprövning av forskning som avser att behandla personuppgifter som antingen är känsliga eller som berör lagöverträdelser m.m. ska det i etikprövningsnämndens prövning ingå att bedöma förutsättningarna för behandlingen av personuppgifter och nämnden ska ange om det ställs krav på samtycke. Om etikprövningsnämnden godkänner en forskningsstudie med särskilda villkor avseende krav på samtycke krävs ett uttryckligt samtycke enligt 15 § personuppgiftslagen från de som deltar i forskningsstudien.

Samtycke och information

Av personuppgiftslagen framgår att ett giltigt samtycke enligt 3 och 15 §§ personuppgiftslagen förutsätter att deltagaren eller deras vårdnadshavare har fått information innan de lämnar sitt uttryckliga samtycke. Samtycket ska vara frivilligt, särskilt, informerat och en otvetydig viljeyttring. Att ett samtycke ska vara särskilt innebär att den enskilde ska informeras om en eller fler

specificerade behandlingar och samtycket ska avse de specifika behandlingarna var för sig. I den information som deltagarna i en forskningsstudie får innan de lämnar sitt samtycke ska det finnas uppgift om den personuppgiftsansvariges identitet. Det innebär att man ska lämna uppgift om namn och kontaktuppgifter beträffande den normalt sett juridiska person som är personuppgiftsansvarig.

I förarbetena till etikprövningslagen uppges även att när forskaren med stöd av ett etikgodkännande enligt etikprövningslagen behandlar personuppgifter har forskaren att följa – förutom de villkor om t.ex. information till deltagarna som har uppställts i samband med etikgodkännandet – bestämmelserna i personuppgiftslagen, t.ex. om rättelse och så kallad registerutdrag (se prop. 2002/03:50 s 119-120). När det gäller rätten att ansöka om registerutdrag enligt 26 § personuppgiftslagen är det lämpligt att det framgår hur en ansökan om information ska göras, dvs. skriftligen hos den personuppgiftsansvarige. Beträffande rätten att få rättelse enligt 28 § personuppgiftslagen anser Datainspektionen att det är lämpligt att det framgår vart den registrerade kan vända sig för att utnyttja sin rättighet.

Tredje lands överföring

I en forskningsstudie måste den personuppgiftsansvarige även följa personuppgiftslagens regler om överföring av personuppgifter till tredje land när forskningen utförs. En överföring till tredje land sker när personuppgifter görs tillgängliga i ett land utanför EU/EES-området. Utgångspunkten är att det är förbjudet att föra över personuppgifter till tredje land om landet inte har en adekvat nivå för skyddet av personuppgifterna, 33 § personuppgiftslagen. Av 34 § personuppgiftslagen framgår att personuppgifter kan överföras till tredje land om den registrerade har gett ett informerat samtycke eller om överföringen är nödvändig i vissa särskilda situationer som anges i den aktuella bestämmelsen. Personuppgifter får också föras över till tredje land om det i annat fall är tillåtet enligt föreskrifter eller särskilda beslut av regeringen eller Datainspektionen, 35 § personuppgiftslagen samt 13-14 §§ personuppgiftsförordningen (1998:1191).

IT-säkerhet

I 31 § personuppgiftslagen ställs krav på att den personuppgiftsansvarige ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de uppgifter som behandlas. Nivån på säkerhetsåtgärder bör klargöras utifrån en risk och sårbarhetsanalys. I bedömningen av lämpligt skydd ska hänsyn tas till

tekniska möjligheter, kostnader, särskilda risker och hur känsliga uppgifterna som behandlas är. Personuppgifter ska skyddas från förstöring genom olyckshändelse eller otillåtna handlingar eller förlust genom olyckshändelse samt mot ändringar, otillåten spridning av eller otillåten tillgång till uppgifterna, särskilt om behandlingen innefattar överföring av uppgifter i ett nätverk, och mot varje annat slag av otillåten behandling.

Vid behandling av känsliga personuppgifter som kommuniceras över öppna nät (t.ex. Internet) ska kommunikationen krypteras på ett sådant sätt att obehöriga inte kan ta del av uppgifterna och åtkomst till de känsliga personuppgifterna ska föregås av stark autentisering. Stark autentisering är en säkerhetsåtgärd som ska tillämpas även om de känsliga personuppgifterna är kodade och kravet gäller för alla användare som har möjlighet att få åtkomst till de kodade personuppgifterna via öppet nät.

Det är Datainspektionen uppfattning att det följer av 31 § personuppgiftslagen att om känsliga personuppgifter lämnas ut över öppet nät, till exempel Internet, får det ske endast till identifierade användare vars identitet är säkerställd med en teknisk funktion såsom asymmetrisk kryptering (t.ex. e-legitimation), engångslösenord eller motsvarande.

Forskningsprojekt CPJMR0092105

Huvudstudien
I avsnittet ”Personuppgiftsansvar” (sid 6) anges följande ”För läkemedelsföretaget Novartis Sverige är personuppgiftsansvarig och kontaktperson den medicinske direktören.” Personuppgiftsansvarig är enligt definitionen i 3 § personuppgiftslagen den person som bestämmer ändamål och medel med behandlingen. Behandlas personuppgifter i en verksamhet så är det den juridiska personen som är personuppgiftsansvarig. Det är således inte verksamhetsansvarig, forskaren eller någon annan anställd som är personuppgiftsansvarig. Datainspektionen anser att det är positivt att Novartis Sverige AB angett en kontaktperson, men att det är missvisande att ange att kontaktpersonen är personuppgiftsansvarig.

Extra framtida forskning
Av patientinformationen framgår att studien består av en huvudstudie och en ”extra framtida forskning”. Det är frivilligt för patienter att delta i endera

studie eller i båda. Patienter kan lämna ett separat samtycke till att delta i den extra framtida forskningsstudien. Vidare framgår att personuppgifterna i den extra framtida forskningsstudien kommer att göras helt anonyma och inte kunna kopplas till patienten. Patienten kan därför inte ta tillbaka sitt samtycke till den extra framtida forskningen när anonymiseringen är genomförd. Av informationen (avsnittet ”Personuppgiftsbehandling” sid 5) anges att ansvarig läkare ansvarar för den kodnyckel som gör det möjligt att koppla uppgifter till patienten. All information som direkt eller indirekt kan hänföras till en fysisk person är en personuppgift enligt 3 § personuppgiftslagen. Kodade uppgifter omfattas därmed också av lagen så länge det finns en kodnyckel bevarad med vars hjälp det är möjligt att identifiera enskilda individer. Det saknar betydelse var och hos vem kodnyckeln förvaras. Så länge kodnyckeln finns kvar är det således personuppgifter i personuppgiftslagens mening. Reglerna i 12 § personuppgiftslagen gällande återtagande av samtycke ska då alltjämt gälla.

Forskningsprojekt CRAD001A2314

Information
För att äldre barn ska kunna lämna ett giltigt samtycke ska informationen innehålla alla nödvändiga uppgifter i enlighet med 25 § personuppgiftslagen och på ett sätt som är begripligt för denna åldersgrupp. Datainspektionen konstaterar att det i informationen till den som är 12-17 år saknas information om vem som är personuppgiftsansvarig och övrig information som behövs för att den registrerade ska kunna ta tillvara sina rättigheter i samband med behandlingen såsom rätten att ansöka om registerutdrag, mottagarna av uppgifterna och rätten att få rättelse i enlighet med vad som angetts ovan.

Avseende båda projekten

Personuppgiftsansvaret

Novartis Sverige AB anför i patientinformationen (sid 6) till studie CPJMR0092105 att det är Västerbotten läns landsting, Umeå universitet samt läkemedelsföretaget Novartis Sverige som är personuppgiftsansvariga samt att studien sponsras av läkemedelsföretaget. Av informationen till vårdnadshavare (sid 5) i studie CRAD001A2314 kan utläsas att ansvariga för genomförande av studien tillika personuppgiftsansvariga är

forskningshuvudmannen Stockholm läns landsting. Från läkemedelsföretaget är Novartis Sverige AB personuppgiftsansvarigt.

Datainspektionen konstaterar att det är svårt att få klarhet i vem som är personuppgiftsansvarig för vad.

För Novartis Sverige AB måste det givetvis stå klart vilken personuppgiftsbehandling som omfattas av Novartis Sverige AB:s personuppgiftsansvar, dvs. för vilken personuppgiftsbehandling bestämmer Novartis Sverige AB ändamålen och medel (se 3 § personuppgiftslagen). Personuppgiftsansvarets omfattning måste också framgå av informationen till patienterna, så att de registrerade kan ta tillvara sina rättigheter i samband med behandlingen så som nämnts ovan.

Av studiesammanfattningen till båda studierna framgår vidare att studieläkaren ger information om studien och inhämtar samtycke till den. Datainspektionen konstaterar att det är otydligt i vilken egenskap som läkaren inhämtar samtycke från patienter och vem läkaren representerar. Tilläggas bör också att om personuppgifter behandlas i en verksamhet så är det den juridiska personen som är personuppgiftsansvarig. Det är således inte verksamhetsansvarig, forskaren eller den så kallade ansvarige läkaren som är personuppgiftsansvarig.

Datainspektionen vill i sammanhanget också påpeka att en vårdgivare måste särskilja uppgifter som omfattas av patientdatalagen från uppgifter som behandlas för forskning. Det är också viktigt att det inte råder någon oklarhet om verksamheternas gränser i förhållande till sekretessreglerna.

Datainspektionen utgår därför från att Novartis Sverige AB klargör omfattningen av personuppgiftsansvaret och gör nödvändiga ändringar i patientinformationen, så att det tydligt framgår för vilken personuppgiftsbehandling Novartis Sverige AB är personuppgiftsansvarig.

Säkerhet vid behandling av personuppgifter

Av det inlämnade materialet kan utläsas att inloggning sker med användarnamn och lösenord. Av materialet kan däremot inte utläsas om användarna behandlar känsliga personuppgifter över öppet nät. Det är Datainspektionen uppfattning att det följer av 31 § personuppgiftslagen att om känsliga personuppgifter lämnas ut över öppet nät, till exempel Internet,

får det ske endast till identifierade användare vars identitet är säkerställd med en teknisk funktion såsom asymmetrisk kryptering (t.ex. e-legitimation), engångslösenord eller motsvarande.

Hur man överklagar

Om ni vill överklaga beslutet ska ni skriva till Datainspektionen. Ange i skrivelsen vilket beslut som överklagas och den ändring som ni begär. Överklagandet ska ha kommit in till Datainspektionen senast tre veckor från den dag ni fick del av beslutet. Datainspektionen sänder överklagandet vidare till Förvaltningsrätten i Stockholm för prövning om inspektionen inte själv ändrar beslutet på det sätt ni har begärt.

Detta beslut har fattats av enhetschefen Katarina Tullstedt efter föredragning av juristen Salomeh Fanaei. Vid den slutliga handläggningen har även it-säkerhetsspecialisten Fredrik Ekman deltagit.

Katarina Tullstedt

Salomeh Fanaei

Kopia till:

NN, samma adress som ovan.
Personuppgiftsombudet NN