Bristol-Myers Squibb AB
Box 1172
171 23 Solna

Tillsyn enligt personuppgiftslagen (1998:204)- två forskningsprojekt vid Bristol-Myers Squibb AB

Datainspektionens beslut

Datainspektionen konstaterar att Bristol-Myers Squibb AB fortsätter att behandla viktiga uppföljningsuppgifter i båda forskningsprojekten även om samtycket återkallats. Datainspektionen förelägger Bristol-Myers Squibb AB att i enlighet med 12 § personuppgiftslagen (1998:204) inte behandla ytterligare personuppgifter om den registrerade återkallat samtycket.

Datainspektionen konstaterar att Bristol-Myers Squibb AB kan komma att anlita en tredje part för att ta reda på en patients kontaktinformation eller nuvarande hälsotillstånd i studierna. Datainspektionen förutsätter att Bristol-Myers Squibb AB följer gällande regler om uppgifterna ska behandlas av tredje part och att personuppgiftsbiträdesavtal upprättas om personuppgifterna behandlas på uppdrag av Bristol-Myers Squibb AB.

Datainspektionen förutsätter att Bristol-Myers Squibb AB uppfyller säkerhetskraven i enlighet med 31 § personuppgiftslagen om känsliga personuppgifter faxas via öppna nät.

Ärendet avslutas.

Bakgrund

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

Datainspektionen begärde därefter att Bristol-Myers Squibb AB skulle lämna en närmare redogörelse för följande forskningsprojekt:

- En fas III, randomiserad dubbelblind studie med BMS-936558 jämfört med dakarbazin hos tidigare obehandlade, inoperabla patienter eller patienter med metastaserande melanom (CA209-066)
- En fas 3, randomiserad dubbelblind studie med enbart Nivolumab eller Nivolumab kombinerat med Ipilimumab hos patienter med tidigare obehandlat inoperabelt eller metastaserande melanom (CA209-067)

Av patientinformationen framgår att syftet med studien CA209-066 är att undersöka effekt, säkerhet och tolerabilitet av nivolumab också kallad BMS-936558 hos patienter med melanom. Läkemedlet nivolumab är ännu inte ett godkänt läkemedel av någon läkemedelsmyndighet för patienter med melanom men är under forskning. Personuppgifter i studien kan komma att i kodad form överföras till USA eller annat land för behandling. Av underlaget i ärendet framgår att deltagarna i forskningsprojektet är över 18 år. Studien är granskad och godkänd av regionala etikprövningsnämnden i Lund.

I patientinformationen för studie CA209-067 anges att syftet med studien är att undersöka effekt och säkerhet av behandling med studieläkemedlet nivolumab ensamt eller då nivolumab kombineras med läkemedlet ipilimumab hos patienter med melanom. Effekten av dessa behandlingar jämförs med effekten hos patienter som endast behandlas med ipilimumab. Nivolumab är ännu inte godkänt läkemedel. De som deltar i studien är över 18 år. Personuppgifter kan i kodad form överföras till USA eller annat land för behandling. Studien är granskad och godkänd av regionala etikprövningsnämnden i Göteborg.

Bristol-Myers Squibb 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.

Skäl för beslutet

Samtycke

Av patientinformationen (CA 209-066 bilaga A sektion 13 sid 8 och CA209-067 sektion 14 sid 8) framgår att om en patient väljer att avbryta studien helt och tar tillbaka sitt samtycke upphör den fortsatta insamlingen av patientens uppgifter, förutom de för studien viktiga uppföljningsuppgifter, t.ex. överlevnadsdata. Om patienten önskar stoppa all vidare insamling av data krävs att patienten anger detta särskilt.

Enligt 12 § personuppgiftslagen har den registrerade rätt att när som helst återkalla ett samtycke. Sedan den personuppgiftsansvarige har mottagit den registrerades återkallelse, får några ytterligare uppgifter om den registrerade inte samlas in eller annars behandlas. Behandling *av redan insamlade uppgifter* får trots återkallelse fortsätta i enlighet med det ursprungligen lämnade samtycket, men uppgifterna får inte uppdateras eller kompletteras. Att fortsätta inhämta nya uppgifter trots att den registrerade återkallat sitt samtycke är inte förenligt med 12 § personuppgiftslagen. Däremot kan uppgifter som redan samlats in behandlas för det ursprungliga ändamålet så länge behandlingen inte strider mot de grundläggande kraven i 9 § personuppgiftslagen. På grund av de grundläggande kraven på kvalitet avseende behandlade personuppgifter enligt 9 § kan det i praktiken innebära att uppgifterna måste utplånas eller avidentifieras när de blivit t.ex. inaktuella eller ofullständiga. Om Bristol-Myers Squibb AB vill behandla viktiga

uppföljningsuppgifter efter att ett samtycke återkallats behöver den registrerade få information om detta och ge sitt frivilliga samtycke till en sådan behandling.

Personuppgiftsbiträde

Det framgår av ingivna handlingar under rubriken ”Frivilligt deltagande/rätt till att avbryta studien” att en tredje part eventuellt kan anlitas för att ta reda på en patients kontaktinformation eller nuvarande hälsotillstånd för det fall att studieläkaren inte får tag på patienten (CA209-066 sektion 13 sid 8 och CA209-067 sektion 14 sid 8). Av informationen framgår inte vilka uppgifter och i vilken egenskap en tredje part agerar i den beskriva situationen. Det är Bristol-Myers Squibb AB:s ansvar att se till att en behandling är förenlig med gällande bestämmelser och om det rör sig om en biträdessituation krävs biträdesavtal med den tredje parten.

Säkerheten vid behandling av personuppgifter

Det framgår av inlagan till Datainspektionen att ”anonyma” personuppgifter faxas till ett centralt laboratorium där de registreras i studiedatabasen. Ur ett säkerhetsperspektiv är kraven på säkerhetsåtgärder högre när känsliga personuppgifter lämnas ut via öppna nät, såsom ofta sker vid faxning. Utifrån personuppgiftslagen har begreppet ”anonymiserade” personuppgifter ingen självständig betydelse. Av information i ärendet framgår att det finns en kodnyckel till uppgifterna. All information som direkt eller indirekt kan hänföras till en fysisk person är en personuppgift. 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 kodnyckel förvaras.

För en verksamhet som regleras av personuppgiftslagen ställs därmed krav på att om känsliga personuppgifter överförs via fax ska den personuppgiftsansvarige vidtagit åtgärder för att försäkra sig om att endast avsedd mottagare får del av uppgifterna samt att överföringen sker krypterat. Kan dessa säkerhetskrav inte uppfyllas ska fax via öppet nät inte användas för att kommunicera känsliga personuppgifterna.

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:

Personuppgiftsombudet NN och NN, samma adress som ovan.