Styrelsen för Stockholms läns
sjukvårdsområde
Box 179 14
118 95 Stockholm

Tillsyn enligt personuppgiftslagen (1998:204) - utlämnande av känsliga personuppgifter

Datainspektionens beslut

Datainspektionen konstaterar att Styrelsen för Stockholms läns sjukvårdsområde (SLSO) behandlat personuppgifter i strid med 4 kap. 1 § och 5 kap. 4 § patientdatalagen genom att ge Medrave AB tillgång till patientuppgifter i syfte att söka fram lämpliga patienter för att delta i ett forskningsprojekt med Karolinska Institutet (KI) som forskningshuvudman.

Datainspektionen förelägger SLSO att tillse att patientuppgifter som behandlas inom hälso- och sjukvården inte lämnas ut för forskningsändamål utan föregående sekretessprövning och att elektronisk tillgång till patientuppgifter inte ges till andra än de som arbetar hos SLSO eller som enligt patientdatalagen tillåts ha direktåtkomst till uppgifterna.

Redogörelse för tillsynsärendet

Tillsynsärendet inleddes efter att Datainspektionen mottagit ett klagomål rörande utlämnande av personuppgifter i samband med en enkätundersökning. Syftet med tillsynen har varit att kontrollera det rättsliga stödet för SLSO:s och Medrave AB:s behandling av personuppgifter i samband med urvalet av personer till enkätundersökningen.

Tillsynen har genomförts skriftligen och genom en inspektion den 12 oktober hos Liljeholmens vårdcentral i Stockholm.

SLSO har i huvudsak uppgett följande. Enkätundersökningen har genomförts som en del av en forskningsstudie som bedrivits av Karolinska Institutet (KI) i egenskap av huvudman, i samarbete mellan Akademiskt primärvårdscentrum och med godkännande av Regionala Etikprövningsnämnden i Stockholm. Tjugofem vårdcentraler har deltagit i studien.

Urvalet av patienter har skett genom att anställda vid företaget Medrave AB på uppdrag av Stockholms läns landstings Hälso- och sjukvårdsförvaltning identifierat patienter utifrån särskilda kriterier. Identifieringen av patienter har skett med hjälp av extraktionsverktyget Medrave 4, som vanligtvis används för kvalitetsuppföljning i vården.

Personnummer för de patienter som valts ut har sedan via en säker anslutning överförts till företaget Indikator som skickat en enkät med följebrev undertecknat av vårdcentralens verksamhetschef med förfrågan till patienterna om de är villiga att delta i studien. De patienter som samtyckt till att delta har fått fylla i en enkät med frågor.

Patienterna har även tillfrågats om godkännande till att vissa uppgifter från journalen samt läkemedelsregisterdata från Socialstyrelsens läkemedelsregister inhämtas och att dessa uppgifter får sambearbetas och ”anonymiseras” så att det inte är möjligt för forskargruppen att identifiera någon enskild person.

Ett begränsat antal variabler från journalen har lämnats ut till registerservice vid Socialstyrelsen för sambearbetning mellan enkätsvar, journaluppgifter och Socialstyrelsens läkemedelsregister. Alla data har därefter ”anonymiserats” och därefter levererats till forskargruppen vid KI i enlighet med Socialstyrelsens rutiner för forskaruttag på det sätt som beskrivits i etikansökan.

Ett andra uttag av personuppgifter från SLSO genomfördes av Medrave AB i ett senare skede i processen, i syfte att göra en bortfallsanalys. Personuppgifterna som då behandlades omfattade samtliga patienter som Medrave AB tagit fram data om, dvs. även patienter som avböjt deltagande och inte gett samtycke till behandling av personuppgifter.

Medrave AB:s mjukvara Medrave 4, som användes för identifieringen av personer för enkätundersökningen, används inom SLSO för

verksamhetsuppföljning m.fl. ändamål enligt patientdatalagen. SLSO har uppgett att det i det aktuella fallet kan ha skett en ändamålsglidning när verktyget användes för att få fram lämpliga patienter till forskningsprojektet.

SLSO har avtalat med Medrave AB om att bolagets personal inte får bereda sig tillträde till den lokala miljön fortsättningsvis. Medrave AB har dock fortfarande teknisk möjlighet att bereda sig åtkomst. Medrave AB behöver inte vara fysiskt uppkopplad mot SLSO:s nätverk för att utnyttja behörigheten, utan företaget kan bereda sig åtkomst till patientuppgifter utifrån, då företaget har extern åtkomst till landstingets nät.

Skäl för beslutet

Avgränsning

Detta tillsynsbeslut avser den behandling av personuppgifter som skett i samband med urvalet av patienter för deltagande i enkätundersökningen för KI:s forskning. I tillsynsbeslutet prövas om de funnits rättsligt stöd för att ge Medrave AB elektronisk tillgång till personuppgifter i vårddokumentationen för att utföra detta urval. Granskningen avser behandlingen som skedde fram till dess att uppgifterna överfördes till Indikator.

Omständigheterna kring biträdesförhållandet mellan Medrave AB och SLSO eller SLSO:s uppdrag till Medrave AB i övrigt är inte föremål för prövning i detta beslut.

Behandling av personuppgifter

Personuppgifter är enligt 3 § personuppgiftslagen all information som direkt eller indirekt kan hänföras till en fysisk person som är i livet. Behandling av personuppgifter är enligt samma paragraf varje åtgärd som vidtas med personuppgifter, t.ex. insamling, lagring och sammanställning.

SLSO har uppgett att Medrave AB tillhandahåller verktyget Medrave 4. Medrave 4 är ett verktyg för att söka fram och sammanställa uppgifter. Inom SLSO används verktyget mot databasen Intelligence. Intelligence är en databas som strukturerats för att underlätta sökning och sammanställning av personuppgifter inom hälso- och sjukvården och som innehåller uppgifter från journalsystemet TakeCare. All nedladdning från Take Care till

Intelligence sker med krypterade personnummer. Medrave AB har dock fått tillgång till nyckeln och har möjlighet att låsa upp krypteringen.

Datainspektionen konstaterar att krypterade uppgifter är personuppgifter så länge det finns möjlighet att genom exempelvis en krypteringsnyckel låsa upp de krypterade uppgifterna, oavsett om den som behandlar personuppgifterna har tillgång till krypteringsnyckeln. Uppgifterna i databasen Intelligence, bland vilka urvalet av patienter till enkätundersökningen skett, utgör därför personuppgifter. Därtill kan konstateras att Medrave AB har möjlighet att låsa upp krypteringen och behandla uppgifterna i klartext.

Personuppgiftsansvar

Enligt 3 § personuppgiftslagen är den som ensam eller tillsammans med andra bestämmer ändamål med och medel för behandling av personuppgifter personuppgiftsansvarig för behandlingen. Enligt 2 § samma lag gäller inte personuppgiftslagen om det i en annan lag eller i en förordning finns bestämmelser som avviker från personuppgiftslagen, utan då ska de avvikande bestämmelserna tillämpas.

Enligt 1 kap. 1 § patientdatalagen ska lagen tillämpas vid vårdgivares behandling av personuppgifter inom hälso- och sjukvården. Enligt 2 kap. 6 § patientdatalagen är en vårdgivare personuppgiftsansvarig för den behandling av personuppgifter som vårdgivaren utför, och i landsting och kommun är varje myndighet som bedriver hälso- och sjukvård personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför.

SLSO har uppgett att SLSO är personuppgiftsansvarig för den behandling av personuppgifter som skett i samband med urvalet av personer för deltagande i enkätundersökningen. SLSO har även uppgett att det är Karolinska Institutet, i egenskap av forskningshuvudman, som är personuppgiftsansvarig för behandlingen av personuppgifter som ägt rum med anledning av den vetenskapliga studien.

Datainspektionen delar bedömningen att SLSO, i egenskap av vårdgivare, är personuppgiftsansvarig i enlighet med patientdatalagens bestämmelse för den behandling av personuppgifter som skett i samband med urvalet av patienter för deltagande i enkätundersökningen och som är föremål för det här tillsynsbeslutet.

Rättslig grund för behandlingen

När är det tillåtet att behandla personuppgifter och känsliga personuppgifter?
All behandling av personuppgifter innebär ett intrång i den personliga integriteten och är bara tillåten om behandlingen har stöd i lag. Enligt personuppgiftslagen är behandling av personuppgifter endast tillåten om den sker med stöd av den registrerades samtycke eller är nödvändig på någon av de grunder som räknas upp i 10 § personuppgiftslagen.

Enligt 13 § personuppgiftslagen är det förbjudet att behandla känsliga personuppgifter i vilket bl.a. ingår personuppgifter som rör hälsa. Undantag från det förbudet kan göras t.ex. om den registrerade lämnat sitt uttryckliga samtycke till behandlingen enligt 15 § personuppgiftslagen, för hälso- och sjukvårdsändamål enligt 18 § personuppgiftslagen och för forskningsändamål enligt 19 § samma lag, om forskningen godkänts efter etikprövning.

Lagligt stöd för behandling av personuppgifter kan även finnas i andra författningar än personuppgiftslagen. Inom hälso- och sjukvårdsverksamhet ger patientdatalagen stöd för, och reglerar, en vårdgivares behandling av personuppgifter inom hälso- och sjukvården.

SLSO:s inställning
SLSO har i huvudsak uppgett följande. Utlämnandet av uppgifter grundar sig på offentlighets- och sekretesslagen plus personuppgiftslagen. Patientdatalagen är givetvis gällande i sin lydelse. Den rättsliga grunden för utlämnandet av personuppgifterna finns i personuppgiftslagen, eftersom behandlingen skedde för forskningsändamål. Forskningen för vilken utlämnandet skedde bedrivs av KI. Patientdatalagen är inte tillämplig på uttaget, utan behandlingen av personuppgifter skedde i enlighet med personuppgiftslagen.

Studien var godkänd av etisk kommitté, både avseende proceduren för inhämtande av patientsamtycke och avseende datauttag för bortfallsanalys för patienter som inte medgett deltagande. Etikgodkännandet är ställt till KI. SLSO lämnade ut personuppgifter i egenskap av vårdgivare. Ett villkor för etikgodkännandet för studien var att berörda patienters samtycke skulle inhämtas.

De berörda patienterna fick information om SLSO:s utlämnande av personuppgifter i och med att de tog emot brevet med enkätundersökningen. Någon information gick inte ut till patienterna före utskicket av enkäten. Samtycke gavs genom att patienterna valde att delta i studien, i och med att de svarade på enkäten. Det framgick av brevet att det fanns en möjlighet att tacka nej till att delta.

Patientdatalagen
Datainspektionen gör följande bedömning av patientdatalagens tillämplighet på den behandling som är föremål för detta tillsynsbeslut. En vårdgivares behandling av personuppgifter inom hälso- och sjukvården regleras av patientdatalagen. SLSO är vårdgivare och de personuppgifter som behandlats för urvalet utgör en del av vårddokumentationen. Patientdatalagen ska därför tillämpas på den aktuella behandlingen.

Ändamål med behandlingen

För att en behandling av personuppgifter ska vara tillåten enligt patientdatalagen måste den som huvudregel ha stöd av något av de tillåtna ändamål som anges i patientdatalagen. Enligt Datainspektionens bedömning omfattas den personuppgiftsbehandling som utförts i samband med beräkning och identifiering av deltagare till enkätundersökningen inte av de ändamål som räknas upp i 2 kap 4 § patientdatalagen.

För myndigheter finns enligt tryckfrihetsförordningen en skyldighet att på begäran och efter erforderlig sekretessprövning tillhandahålla allmänna handlingar. Myndigheter kan även ha en uppgiftsskyldighet gentemot andra myndigheter. Den behandling av personuppgifter som är nödvändig för sådana utelämnanden kan ske med stöd av 2 kap. 5 § patientdatalagen, där det anges att personuppgifter som behandlas för ändamål som anges i 2 kap. 4 § även får behandlas för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning.

Datainspektionens konstaterar mot denna bakgrund att en offentlig vårdgivares behandling av personuppgifter som är insamlade med stöd av de ändamål som anges i 2 kap. 4 § patientdatalagen och som är nödvändig för att tillmötesgå en begäran om att få del av allmän handling eller på grund av annan uppgiftsskyldighet kan ske med stöd av 2 kap. 5 § patientdatalagen.

Vid det urvalsförfarande som ägt rum har SLSO gett en extern aktör åtkomst till databasen med patientuppgifter för att söka efter patienter av intresse för den aktuella forskningen. Det kan konstateras att SLSO har utlämnat uppgifterna när Medrave AB fått tillgång till uppgifterna i databasen Intelligence. Den behandling som sker hos Medrave AB kan därmed inte anses ske i syfte att SLSO ska fullgöra en uppgiftsskyldighet eller utlämna allmänna handlingar enligt offentlighets- och sekretesslagen.

Enligt 2 kap. 5 § patientdatalagen gäller den så kallade finalitetsprincipen i 9 § första stycket d personuppgiftslagen som anger att personuppgifter inte får behandlas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in. När det gäller behandling av personuppgifter för vetenskapliga ändamål så ska sådan behandling inte anses som oförenlig med de ändamål för vilka uppgifterna samlades in enligt 9 § andra stycket personuppgiftslagen.

Det kan även noteras att behandling av personuppgifter enligt 2 kap. 3 § patientdatalagen kan vara tillåten för andra ändamål än de som anges i samma lag, om den enskilde lämnat ett uttryckligt samtycke till behandlingen. För att ett samtycke ska vara giltigt krävs att samtycket lämnas innan behandlingen inleds, vilket inte skett i det aktuella fallet.

Behandling med stöd av personuppgiftslagen
Datainspektionen gör följande bedömning av personuppgiftslagens tillämplighet på den behandling av personuppgifter som är föremål för detta beslut.

I propositionen till patientdatalagen görs bl.a. följande uttalanden rörande behandling av patientuppgifter för forskningsändamål. Det är tillåtet att behandla patientuppgifter som samlats in i hälso- och sjukvårdens individinriktade verksamhet om den registrerade lämnat sitt uttryckliga samtycke till behandlingen eller om behandlingen har godkänts enligt lagen (2003:460) om etikprövning av forskning som avser människor. Om uppgifterna samlats in hos en hälso- och sjukvårdsmyndighet krävs därutöver, om forskningen bedrivs som en självständig verksamhetsgren inom myndigheten eller av en extern forskningshuvudman, att en sekretessprövning gett vid handen att uppgifterna kan lämnas ut till forskningsverksamheten. Vid forskning som bedrivs integrerat med vården av

patienten är patientdatalagen tillämplig rörande den personuppgiftsbehandling som rör vården (prop. 2007/08:126, s 203)

Det kan mot denna bakgrund konstateras att den personuppgiftsbehandling som en vårdgivare vidtar för forskningsändamål regleras av personuppgiftslagen, med undantag för sådan forskning som sker integrerat med vården av patienten. Innan uppgifterna lämnas ut för forskning, antingen hos vårdgivaren i en annan verksamhetsgren eller hos en extern forskningshuvudman, måste en sekretessprövning vidtas.

I det aktuella fallet är det själva urvalet av patientuppgifter som är föremål för granskning. I det skedet är det fråga om patientuppgifter som behandlas av vårdgivaren med stöd av patientdatalagen och något uttag av uppgifterna har ännu inte skett. Den aktuella behandlingen kan därför inte genomföras med stöd av personuppgiftslagen.

Behandling med stöd av samtycke
SLSO har uppgett att samtycke inhämtades först efter att den behandling av personuppgifter som urvalet innebar hade genomförts. För att ett samtycke ska kunna utgöra grund för en behandling av personuppgifter krävs det att samtycket lämnas innan behandlingen inleds.

Det har inte framkommit att SLSO tillfrågat de patienter bland vars personuppgifter urvalet skedde om de samtyckt till den behandling av personuppgifter som urvalet och sammanställningen av personuppgifter inneburit. Datainspektionen bedömer därför att samtycke inte utgör en giltig grund för den behandling av personuppgifter som är föremål för detta beslut.

Åtkomst till och utlämnande av uppgifter enligt patientdatalagen

Tillåtna former av elektronisk tillgång till vårdgivarens vårddokumentation regleras uttömmande i patientdatalagens 4, 5 och 6 kap.

Elektronisk åtkomst inom ramen för den inre sekretessen
Enligt 4 kap. 1 § patientdatalagen får den som arbetar hos en vårdgivare ta del av dokumenterade uppgifter om en patient endast om han eller hon deltar i vården av patienten eller av annat skäl behöver uppgifterna för sitt arbete inom hälso- och sjukvården.

SLSO har uppgett att personalen hos Medrave AB som utförde den behandling av personuppgifter som är föremål för detta beslut inte hade någon anställning hos SLSO när behandlingen ägde rum. De anställda hos Medrave AB har inte heller haft ett direkt uppdrag hos SLSO utan uppdraget har ålegat den juridiska personen Medrave AB. Det har inte framkommit att personalen som utförde behandlingen på annat sätt varit knuten till SLSO på ett sådant vis att personalen kan anses ha ingått i myndighetens organisation och befunnit sig inom sekretessområdet på det sättet som avses i 2 kap. 1 § offentlighets- och sekretesslagen (2009:400).

Eftersom personalen vid Medrave AB inte arbetat hos SLSO så har åtkomst till uppgifterna inte kunnat ske med stöd av bestämmelsen om elektronisk åtkomst inom ramen för den inre sekretessen enligt 4 kap. 1 § patientdatalagen.

Utlämnande genom direktåtkomst
Utlämnande genom direktåtkomst till personuppgifter som regleras av patientdatalagen är enligt 5 kap. 4 § samma lag tillåten endast i den utsträckning som anges i lag eller förordning. Bestämmelsen i 5 kap. 5 § patientdatalagen reglerar patientens direktåtkomst till sina egna uppgifter och i lagens sjätte kapitel regleras en vårdgivares direktåtkomst till uppgifter hos en annan vårdgivare inom ramen för sammanhållen journalföring.

Medrave AB är varken patient eller vårdgivare och omfattas därför inte av patientdatalagens regler om tillåten direktåtkomst. Behandlingen som är föremål för detta beslut har därför inte kunnat ske med stöd av patientdatalagens bestämmelser om tillåten direktåtkomst.

Utlämnande på medium för automatiserad behandling
Enligt 5 kap. 6 § patientdatalagen kan en uppgift som får lämnas ut, lämnas ut på medium för automatiserad behandling. Ett sådant utlämnande förutsätter en aktivitet hos den personuppgiftsansvarige, innefattande bl.a. en sekretessprövning, som inte ägt rum här.

SLSO:s uppgifter
Avseende de bedömningar som gjorts ifråga om sekretess enligt offentlighets- och sekretesslagen har SLSO uppgett följande. Upplägget bygger på att samtycke inhämtas från berörda försökspersoner. Uppgifter till berörda personer hos Medrave AB har lämnats med förbehåll enligt 10 kap. 14 § första

stycket och 12 kap. 2 § andra stycket OSL. Företaget har personuppgiftsbiträdesavtal med SLSO och individuella sekretessförbindelser för personer som hanterat uppgifterna.

Avseende förfarandet för urval av personer till enkätstudien har SLSO uppgett i huvudsak följande. Medrave AB gick inte in i Take Care utan i den databas, dvs. Intelligence, där uppgifterna från Take Care lagras. Personalen vid Medrave AB har haft behörighet att på egen hand komma åt uppgifter i databasen Intelligence och göra sitt eget urval till uppdraget inom ramen för forskningsprojektet, för att sedan plocka ut och hämta hem uppgifterna. Det ingår i Medrave AB:s avtal med SLSO att bolaget ska leverera Medrave 4. Medrave AB måste i detta syfte ha full tillgång till uppgifterna i Medrave 4. Detta innebär att bolagets personal kan se alla personnummer och även en lista över personnummer. Det är också så det måste ha gått till inom ramen för projektet. Vid sökning mot databasen Intelligence användes sökord som angav viss diagnos eller visst recept. Medrave AB kunde välja vilken information som skulle sökas fram och visas, och se den data som företaget självt paketerat. Det rörde sig om personuppgifter som finns i journalerna. Om Medrave AB inte hade haft full behörighet hade det inte varit möjligt att söka och sammanställa dessa uppgifter. Medrave AB:s åtkomstmöjlighet innebar inte någon direktåtkomst till journalerna i Take Care.

Datainspektionens bedömning
Datainspektionen konstaterar att det av de uppgifter SLSO lämnat i ärendet skriftligen och vid inspektionstillfället framgår att personalen vid Medrave AB getts tillgång till uppgifter i vårdgivarens vårddokumentation utan föregående sekretessprövning. Vad som framkommit visar enligt Datainspektionens bedömning att åtkomst inte bara getts till uppgifter rörande de personer som sedermera valts ut att ingå i enkätundersökningen, utan till samtliga uppgifter bland vilka uppgifterna om utvalda personerna ingått. Behandlingen av uppgifter har således inte enbart omfattat personer som ingått i enkätundersökningen och som sedermera erhållit information och tillfrågats om samtycke.

Det har förvisso inte rört sig om direktåtkomst till personuppgifter i journalsystemet Take Care, men om tillgång till patientuppgifter som ingår i vårdgivarens vårddokumentation i databasen Intelligence och tillgången har getts utan föregående sekretessprövning. Syftet för utlämnandet har varit att sedermera utlämna kodade patientuppgifter efter samtycke till KI.

Datainspektionen konstaterar sammanfattningsvis att Medrave AB:s tillgång till patientuppgifter inte varit fråga om ett lagenligt utlämnande av personuppgifter på medium för automatiserad behandling enligt 5 kap. 6 § patientdatalagen. Det har inte heller varit fråga om tillåten elektronisk åtkomst enligt 4 kap. patientdatalagen eller tillåten direktåtkomst enligt 5 och 6 kap. samma lag till patientuppgifter, utan en direktåtkomst till uppgifter som saknar stöd i lag.

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 beslutet meddelades. 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 generaldirektören Kristina Svahn Starrsjö efter föredragning av juristen Eva Maria Broberg. Vid den slutliga handläggningen har även enhetschefen Katarina Tullstedt deltagit.

Kristina Svahn Starrsjö

Eva Maria Broberg

Vid den slutliga handläggningen av ärendet har även it-säkerhetsspecialisten Magnus Bergström deltagit.

Kopia till:

Personuppgiftsombuden (för kännedom)