Chefsjustitieombudsmannen
Elisabeth Rynning

Kritik mot Region Halland för att ha lämnat ut personuppgifter till tredje land i strid med gällande lagstiftning m.m.

Beslutet i korthet: Region Halland lämnade inom ramen för ett utvecklingssamarbete med Brigham and Women's Physicians Organization Inc. (BWPO), med säte i USA, i april 2016 ut uppgifter ur patientjournaler till BWPO. Uppgifterna lämnades ut utan patienternas namn och personnummer men med angivande av ett löpnummer för varje patient (pseudonymisering). Patienternas personnummer och löpnummer bevarades i en referensfil som inte lämnades ut till BWPO.

ChefsJO uttalar inledningsvis att uppgifter ur patientjournaler typiskt sett är information som är mycket känslig ur integritetssynpunkt och som inom hälso- och sjukvården skyddas genom dels bestämmelser om hur personuppgifter får behandlas, dels bestämmelser om sekretess och tystnadsplikt. ChefsJO framhåller vidare att utvecklingsarbete som utförs på vetenskaplig grund och innefattar behandling av känsliga personuppgifter kräver etikgodkännande, men har vid granskningen av dessa ärenden utgått från att det aktuella samarbetet enbart har innefattat annat kvalitets- och utvecklingsarbete.

I beslutet konstaterar chefsJO att de uppgifter som lämnades ut till BWPO inte var helt avidentifierade eftersom det med hjälp av referensfilen fortfarande var möjligt att identifiera enskilda individer. Uppgifterna var därmed att anse som personuppgifter. ChefsJO slår därefter fast att kraven i personuppgiftslagen för överföring av personuppgifter till tredje land inte var uppfyllda vid utlämnandet till BWPO. Regionen kritiseras för att ha lämnat ut personuppgifter i strid med då gällande lagstiftning.

När det gäller frågan om utlämnandets förenlighet med sekretesslagstiftningen konstaterar chefsJO att pseudonymisering i sig kan medföra att det saknas risk för att en enskild person ska lida skada eller men, och att uppgifterna därmed kan lämnas ut. Det är emellertid viktigt att en myndighet även vid utlämnande av uppgifter i pseudonymiserad form gör en noggrann sekretessprövning utifrån förhållandena i varje enskilt fall. I det här fallet fanns flera omständigheter som chefsJO anser borde ha manat till försiktighet, bl.a. att utlämnandet avsåg uppgifter som dels var av mycket integritetskänsligt slag, dels rent generellt kan underlätta identifiering av enskilda individer. I vilken utsträckning det faktiskt har varit möjligt att identifiera enskilda individer har inte kunnat klarläggas genom utredningen. Enligt chefsJO:s mening framstår det dock inte som osannolikt att s.k. bakvägsidentifikation i vissa fall skulle ha varit möjlig. ChefsJO konstaterar att utlämnandet inte tycks ha föregåtts av någon egentlig sekretessprövning hos regionen och är därför kritisk till hanteringen. Regionen kritiseras även för bristande dokumentation i ärendet.

Anmälningarna

I två anmälningar som kom in till JO den 9 oktober 2017 (dnr 6794-2017) och den 12 oktober 2017 (dnr 6864-2017) framförde AA och BB klagomål mot Region Halland och anförde i huvudsak följande:

Region Halland har ett pågående forskningssamarbete med Brigham and Women's Hospital i Boston. Regionen har skickat känsliga uppgifter ur patientjournaler till USA utan att det mottagande sjukhuset tecknat något sekretessavtal. Regionen har inte heller informerat berörda patienter.

Utredning

Anmälningarna remitterades till Region Halland, regionstyrelsen, för yttrande. I sitt remissvar anförde regionstyrelsen i huvudsak följande:

Omständigheter

För att möta hälso- och sjukvårdens framtida utmaningar har Region Halland sedan 2015 bedrivit ett omfattande förändringsarbete av hälso- och sjukvården i Hallands län benämnt Framtidsarbetet.

Ur Framtidsarbetets inledande analyser drogs slutsatsen att det fanns ett stort behov av en mer långsiktig strategi för hälso- och sjukvården i Region Halland. Framtidsarbetet och de slutsatser som dragits i detta arbete ligger till grund för Region Hallands hälso- och sjukvårdsstrategi för perioden 2017–2025 och som antogs av Regionfullmäktige i november 2016. Strategin har ett flertal fokusområden, bl.a. ska regionens hälso- och sjukvård präglas av flödes- och resurseffektivitet samt skapa goda förutsättningar för patientnära forskning vars resultat ska integreras i det löpande arbetet.

Som ett led i Region Hallands förbättringsarbete bedriver regionen – liksom andra landsting och regioner – analyser på vårddata i verksamheten. Ett problem är att regionen förfogar över en stor mängd olika data, men besitter inte själv fullt ut den expertis som krävs för att utnyttja denna kunskap i form av analyser av vårdflöden, behandlingsmetoder och kostnader per patient över tid. För att kunna utveckla kvalitén i vården finns ett behov av att kunna analysera fakta på gruppnivå.

Den 29 januari 2016 beslutade därför regionstyrelsen i Region Halland om att godkänna tecknandet av ett flerårigt samarbetsavtal med Brigham and Women's Hospital i Boston, USA, gällande forskning och utveckling, att uppdra åt regionstyrelsens ordförande att teckna avtalet och att resultatet av samarbetet ska återredovisas till regionstyrelsen fortlöpande.

Samarbetsavtal tecknades sedermera den 2 februari 2016 mellan Region Halland och Brigham and Women's Physicians Organization Inc. (BWPO). BWPO är den juridiska person som ansvarar för verksamheten vid sjukhuset Brigham and Women's Hospital i Boston (BWH), USA. Samarbetet sträcker sig enligt avtalet t.o.m. 2 februari 2019. Av avtalet framgår bl.a. att parterna ska iaktta tystnadsplikt avseende alla uppgifter inom ramen för samarbetet.

Det finns flera anledningar till att Region Halland har valt att samarbeta med BWPO. BWPO har lyckats väl i sitt utvecklingsarbete av BWH:s verksamhet, och det finns många likheter med den förändringsresa Region Halland behöver göra. BWPO har optimerat sin akutsjukvård och genomfört de förändringar i arbetssätt som Region Halland har framför sig. BWH rankas vidare som en av USA:s topp tio sjukhus, liksom bland akutsjukhus. Sjukhuset har också en erkänt högkvalitativ forskning som kan stimulera till ökad forskning och höjd kunskapsnivå i Halland. Sjukhuset samarbetar med bl.a. Harvard Medical

School. Samarbetet har av regionstyrelsen bedömts, kort sagt, vara förenligt med och nödvändigt för regionens långsiktiga hälso- och sjukvårdsstrategi (se ovan).

Det övergripande syftet med samarbetet är att ”optimize the level of care and at the same time increase quality of care, reduce costs and increase the patient satisfaction.” I korthet stipulerar samarbetsavtalet följande gemensamma arbete:

1) Utveckla metoder för att analysera de data som redan finns i Region Halland.

2) Utveckling av akutprocessen med syfte att förbättra akutvården i Halland.

3) Skapa utökade möjligheter till forskning inom Region Halland.

I det följande uppehåller sig yttrandet vid punkten 1 ovan (”Utveckla metoder för att analysera de data som redan finns i Region Halland”).

Som framhållits är flödes- och resurseffektivitet ett av fokusområdena i Region Hallands hälso- och sjukvårdsstrategi för att optimera tillgängliga resurser. Vad som avses här är analyser av hälso- och sjukvårdens flöden på systemnivå, identifiera problemområden och kunna förutse vilka effekter olika åtgärder kan ge. Det kan handla om att identifiera t.ex. inadekvat läkemedelsbehandling av vissa diagnoser, bristande uppföljning av utskrivna patienter från den slutna vården, t.ex. vid akutsjukvård, eller hälsorelaterade (dolda) risker som inte uppmärksammas i tillräcklig hög grad, t.ex. hjärtsvikt samt komplext sjuka patienter. Identifieringen av sådana brister i verksamheten kan ske medelst datorsimuleringar baserade på tillgängliga data. Som referenser för att hitta ”flaskhalsar” och avvikelser kan man använda riktlinjer för vård, t.ex. Socialstyrelsens nationella riktlinjer, eller jämförelsetal från Nationella Kvalitetsregister.

En anledning till att Region Halland inledde ett samarbete med BWPO inom forskning och utveckling på hälso- och sjukvårdens område är att BWPO besitter en unik kompetens inom flödes- och resurseffektivitet och datorsimulering. Det stod därför tidigt klart i samarbetet mellan Region Halland och BWPO att BWPO skulle bygga upp en data- och simuleringsmiljö för sådana analyser åt regionen – på plats i Halland. Denna data- och simuleringsmiljö, benämnd SHARP (Strategisk HälsoAnalysPlattform) färdigställdes i november 2016. SHARP bygger i stort på de metoder och analysverktyg som BWPO själva använder.

För att kunna bygga SHARP krävdes en ingående analys av befintliga data i olika vårdadministrativa system som regionen förfogade själv över. Det förutsatte, enkelt uttryckt, ett förarbete i form av en ”kartläggning” av befintliga typer av data, datastrukturer, dataflöden och vårdprocesser inom regionens hälso- och sjukvårdsverksamhet. Sådana analyser behövde dessutom göras på individuella patientflöden. Eftersom analysverktyg och tillgänglig datakompetens fanns i BWPO:s datacenter i Boston, övervägdes ett utlämnande av data från Region Hallands hälso- och sjukvårdsproduktion för 2015 till BWPO.

Under februari–april 2016 bedrevs inom regionkontoret ett förberedande arbete att sammanställa data för BWPO:s analys. En central fråga under beredningen utgjorde skyddet för enskilda individers uppgifter om hälsa och personliga förhållanden och de rättsliga förutsättningarna för att kunna lämna ut uppgifterna.

Eftersom känsliga uppgifter skulle överföras till en mottagare i ett annat land och regionen skulle få en sämre kontroll över uppgifterna, fördes diskussioner bland berörda medarbetare på regionkontoret vilka variabler (uppgifter) som skulle kunna lämnas ut för att uppnå tillräcklig kvalitet i analysarbetet utan att samtidigt röja enskilda individer. Det bestämdes att uppgifterna skulle lämnas utan angivande av namn och personnummer, men med ett löpnummer för varje grupp om uppgifter per individ för att särskilja data mellan individer. Därmed var

bedömningen att varken offentlighets- och sekretesslagstiftningen eller persondataskyddsregleringen blir tillämplig på utlämnandet.

Det bestämdes att datauttaget skulle omfatta 18 variabler. Förutom variabler om bl.a. diagnos, labbsvar, läkemedelsanvändning och vårdenhet på individnivå fanns även uppgift om födelseår och bosättningskommun. Inga namn eller personnummer förekom. Varje patients data åsattes ett löpnummer (1, 2, 3 osv.) för att särskilja individer i datauttaget. Varje patients löpnummer och personnummer bevarades i en fil som enbart tre medarbetare på Region Halland och tre konsulter i Region Hallands upphandlade konsultavtal (som arbetar med analysmiljön) samt Region Hallands anställda databasadministratörer på it-service hade teknisk tillgång till via sina administratörsrättigheter. Denna ”nyckel” lämnades inte ut till BWPO. Filen var en referenspunkt vid eventuella behov av kontroll av dataanalyser, eventuella uppdateringar av data till analysmiljön från källsystemen. I efterhand kan konstateras att diskussionerna och ställningstaganden internt om utelämnandet borde ha dokumenterats i form av minnesanteckningar o dyl.

Den 19 april 2016 beslutade dåvarande chefen för enheten för uppdrag och analys, att lämna ut data till BWPO. Uppgifterna överfördes till BWPO i en krypterad fil över internet på en krypterad förbindelse. Detta beslut fattades med utgångspunkt i ovan beskrivna rutin.

Beslutet skedde enligt gällande delegationsordning för regionstyrelsen. Vilket säger att ”beslut om utlämnande av patientuppgifter från vårdinformationssystem eller databaser för verksamhetsuppföljning, kvalitetssäkring och forskning kan beslutas av chefen för forskning och utvecklingsenheten”. Då ordinarie beslutsfattare vid tillfället var frånvarande fattades beslutet av dennes ersättare, dvs. chefen vid uppdrag och analys.

Gällande rätt

Region Halland är rättsligt sett ett landsting. Bestämmelser om landsting finns bl.a. i kommunallagen (1991:900). Landstingen har enligt hälso- och sjukvårdslagen (2017:30; HSL) ett omfattande ansvar på hälso- och sjukvårdens område och ska på ett övergripande plan erbjuda en god hälso- och sjukvård åt dem som är bosatta inom länet samt verka för en god hälsa hos hela befolkningen.

I landstingens planeringsansvar ingår enligt HSL bl.a. att planera hälso- och sjukvården med utgångspunkt i befolkningens behov av sådan vård (7 kap. 2 §). Planeringen ska även avse den hälso- och sjukvård som bedrivs av privata och andra vårdgivare. Det är fråga om ett ”totalansvar”.[1] Det ansvaret inkluderar också i samhällsekonomiska lägen med begränsad resurstillväxt att planeringen i den offentliga hälso- och sjukvården inriktas mot att kostnaderna ska kunna hållas nere.[2]

Bestämmelser om behandling av personuppgifter finns i personuppgiftslagen (1998:204; PUL). Syftet med lagen är att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter. Personuppgiftslagen är ett genomförande i svensk rätt av EU:s

[1] Lars-Åke Johnsson. Kommentar till hälso- och sjukvårdslagen. Zeteo. Kommentaren till 7 kap. 2 § HSL.

[2] Prop. 1981/82:97 s. 61 f.

dataskyddsdirektiv. Den 25 maj 2018 upphör PUL och dataskyddsdirektivet och ersätts av en ny europeisk dataskyddsförordning samt en ny dataskyddslag och brottsdatalag.

Begreppet ”personuppgifter” är hämtat från PUL. Med personuppgift avses i PUL all information som direkt eller indirekt kan hänföras till en fysisk person som är i livet (3 §). Det uppställs således inga kvalitetskrav på informationen för att lagen ska bli tillämplig, t.ex. att det ska vara fråga om vissa särskilt privata eller känsliga uppgifter. Det är tillräckligt att det är fråga om information som kan hänföras till en viss identifierbar individ.

För att avgöra om en person är identifierbar ska alla hjälpmedel beaktas som i syfte att identifiera vederbörande rimligen kan komma att användas av antingen den som är ansvarig för behandlingen (den personuppgiftsansvarige) eller av någon annan person. Begreppet personuppgift omfattar vidare all information om individer, oavsett deras ställning eller kapacitet.

Även pseudonymiserade personuppgifter, t.ex. krypterade personuppgifter eller andra liknande elektroniska identifikationsinstrument, kan utgöra personuppgifter. Om de kan ”dekrypteras” med en kodnyckel, översättnings-tabell eller andra medel utgör de personuppgifter. Det är inte nödvändigt att en identifikation har skett för att det ska kunna vara fråga om en personuppgift. Det är fullt tillräckligt att så kan komma att ske.

Det finns ett flertal situationer där PUL inte är tillämplig. T.ex. gäller inte lagen för sådan behandling av personuppgifter som en fysisk person utför som ett led i en verksamhet av rent privat natur (6 §). Som exempel kan nämnas privatpersoners ord- och textbehandling, privat korrespondens med e-post och privat inspelning med digitalkamera i hemmet. Lagen är inte heller tillämplig på hantering av uppgifter som är helt avidentifierade, dvs. som inte kan bakåtspåras eller indirekt hänföras till en fysisk levande person.

Utgångspunkten i PUL är att alla former av behandlingar av personuppgifter som på något sätt är strukturerade är förbjudna. Lagen tillåter emellertid en juridisk eller fysisk person, en personuppgiftsansvarig, att i vissa fall få behandla personuppgifter. Sådana lagliga grunder för personuppgiftsbehandling finns i 10 § PUL. Samtycke är en sådan laglig grund, liksom t.ex. avtal med den registrerade eller arbetsuppgifter av allmänt intresse för att nämna några exempel.

Behandling av personuppgifter i en ostrukturerad form som inte påtagligt underlättar sammanställning eller sökning av personuppgifter, t.ex. i e-post eller på en Facebooksida, är också tillåten enligt PUL, oavsett ändamål, förutsatt att behandlingen inte är kränkande för de personer vars personuppgifter behandlas (5 a §).

Beträffande känsliga personuppgifter finns också bestämmelser i PUL. Som känsliga personuppgifter betraktas bl.a. uppgifter om ras, etnicitet, religionstillhörighet och hälsa (13 §). Utgångspunkten är att det råder ett förbud för att behandla känsliga personuppgifter, såvida inte det finns en laglig grund. Vilka dessa lagliga grunder är framgår av 15–19 §§ PUL. En sådan laglig grund är hälso- och sjukvård (18 §). Därutöver får den som är yrkesmässigt verksam inom hälso- och sjukvårdsområdet och har tystnadsplikt behandla känsliga personuppgifter som omfattas av tystnadsplikten.

PUL innehåller också bestämmelser om grundläggande krav på behandling av personuppgifter (9 §) som alltid måste vara uppfyllda, oavsett om behandlingen grundas på den registrerades samtycke eller en annan laglig grund. Som exempel kan nämnas kraven på att behandlingen är laglig, att den sker i enlighet med god sed samt att ändamålen är särskilda, uttryckligt angivna och berättigade.

Enligt 31 § ska den personuppgiftsansvarige också vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Om den personuppgiftsansvarige anlitar ett personuppgiftsbiträde, dvs. osjälvständig

aktör utanför den personuppgiftsansvariges organisation som behandlar personuppgifter för den personuppgiftsansvariges räkning enligt instruktion, ska ett avtal tecknas härom.

PUL är emellertid subsidiär i förhållande till annan författning, dvs. om det i en annan lag eller i en förordning finns bestämmelser som avviker från lagen, ska de bestämmelserna gälla (2 §). En sådan lag är patientdatalagen (2008:355).

När vårdgivare behandlar personuppgifter inom hälso- och sjukvården gäller patientdatalagen (PDL). Med vårdgivare avses enligt 1 kap. 3 § PDL statlig myndighet, landsting och kommun i fråga om sådan hälso- och sjukvård som myndigheten, landstinget eller kommunen har ansvar för (offentlig vårdgivare) samt annan juridisk person eller enskild näringsidkare som bedriver hälso- och sjukvård (privat vårdgivare). Region Halland är i grund och botten ett landsting som bedriver bl.a. hälso- och sjukvård. Region Halland är således en vårdgivare.

PDL tar dock inte helt över PUL. PDL är en specialreglering, och om inte annat framgår av PDL så gäller PUL. Åtskilliga bestämmelser i PUL kan alltså bli tillämpliga vid personuppgiftsbehandling i hälso- och sjukvården. Vidare gäller t.ex. PUL:s bestämmelser om säkerhet i 30–32 §§ och om överföring av personuppgifter till tredje land i 33–35 §§.

l sammanhanget kan även nämnas att Socialstyrelsen, med stöd av patientdataförordningen (2008:360), meddelat föreskrifter och allmänna råd (HSLF-FS 2016:40) om journalföring och behandling av personuppgifter i hälso- och sjukvården som på en rad områden preciserar och fyller ut bestämmelserna i PDL och PUL.

l 2 kap. PDL finns grundläggande bestämmelser. Där framgår för vilka ändamål en vårdgivare får behandla personuppgifter utan patientens samtycke (4 §). Förutom individuell vård och behandling får en vårdgivare behandla känsliga personuppgifter om hälsa för bl.a. ändamålen systematisk och fortlöpande utvärdering, uppföljning och kvalitetssäkring. Som redovisas ovan har en vårdgivare en skyldighet enligt HSL att följa upp och förbättra kvaliteten i vården. Vidare får en vårdgivare behandla personuppgifter för statistiska ändamål. En patient får enligt PDL spärra sina uppgifter vid en vårdenhet eller en vårdprocess inom en vårdgivares verksamhet så att de inte är elektroniskt åtkomliga för personal vid andra vårdenheter eller vårdprocesser (4 kap.). Sådana spärrar behöver dock inte beaktas av en vårdgivare om uppgifterna behövs för systematisk utvärdering, uppföljning eller kvalitetssäkring.

Bestämmelser om patientjournaler är samlade i 3 kap. Med patientjournal avses enligt lagen en eller flera journalhandlingar, som rör samma patient, och med journalhandling avses framställning i skrift eller bild samt upptagning som kan läsas, avlyssnas eller på annat sätt uppfattas endast med tekniskt hjälpmedel och som upprättas eller inkommer i samband med vården av en patient och som innehåller uppgifter om patientens hälsotillstånd eller andra personliga förhållanden eller om vidtagna eller planerade vårdåtgärder (1 kap. 3 §).

Syftet med att föra en patientjournal är, enligt PDL, i första hand att bidra till en god och säker vård av patienten (3 kap. 2 §). Journalen är ett stöd för den eller de personer som ansvarar för vården av patienten, men den är även en informationskälla för patienten. Av förarbetena till lagen framgår vidare att journalen också är ett viktigt instrument för vårdgivarens egenkontroll samt i kvalitets-, säkerhets-, uppföljnings- och utvärderingsarbete. Inte sällan har patientjournalen även betydelse i olika juridiska sammanhang, exempelvis i samband med Inspektionen för vård och omsorgs (IVO) verksamhets- och individtillsyn och ärenden i Hälso- och sjukvårdens ansvarsnämnd (HSAN).

l 6 kap. PDL finns bestämmelser om s.k. sammanhållen journalföring. Regleringen innebär att vårdgivare under vissa förutsättningar kan få direktåtkomst till varandras elektroniska journalhandlingar och andra personuppgifter. En väsentlig förutsättning för direktåtkomst är dock att

uppgifterna behövs för individuell vård och behandling eller utfärdande av intyg. Direktåtkomst för andra ändamål, t.ex. systematisk uppföljning eller utvärdering, är inte tillåtet enligt lagen.

PDL innehåller inte någon särskild reglering om överföring av personuppgifter till tredje land utan i dessa delar gäller PUL:s bestämmelser för en vårdgivare. Med tredje land avses enligt PUL en stat som inte ingår i Europeiska unionen eller är ansluten till EES-avtalet. Eftersom det inte finns några universella generella regler som ger motsvarande garantier för persondataskyddet för européer utanför EU/EES-området begränsar dataskyddsdirektivet överföring av européers personuppgifter till tredje länder. Dessa begränsningar finns i 33–35 §§ PUL.

En vårdgivare som avser att överföra patientuppgifter till en mottagare i utlandet måste således först avgöra huruvida den behandling som överföringen innebär (utlämnandebehandlingen) är laglig i sig, och därefter bedöma vad som krävs för en överföring till ett specifikt tredje land. Vid laglighetsbedömningen ska även sekretess- och tystnadspliktsbestämmelser beaktas.

Som huvudregel gäller ett förbud mot att lämna ut personuppgifter till länder utanför EU eller EES (33 § PUL). Förbudet får dock sättas åt sidan av den personuppgiftsansvarige i vissa fall som framgår närmare av 33 § andra stycket, 34 § och 35 § PUL. Personuppgifter får överföras till tredje land om mottagarlandet har en adekvat skyddsnivå. Frågan om en skyddsnivå är adekvat skall bedömas med hänsyn till samtliga omständigheter som har samband med överföringen. Särskild vikt ska läggas vid uppgifternas art, ändamålet med behandlingen, hur länge behandlingen skall pågå, ursprungslandet, det slutliga bestämmelselandet och de regler som finns för behandlingen i det tredje landet. Regeringen får emellertid meddela föreskrifter om undantag från förbudet i 33 § för överföring av personuppgifter till vissa stater. Regeringen får också meddela föreskrifter om att överföring av personuppgifter till tredje land är tillåten, om överföringen regleras av ett avtal som ger tillräckliga garantier till skydd för de registrerades rättigheter. Vilka dessa stater är framgår av bilaga 1 till personuppgiftsförordningen (1998:1191).

Vidare får överföring ske till tredje land om den registrerade gett sitt samtycke till överföringen, om det är nödvändigt i vissa fallsituationer som finns uppräknade i 34 § PUL, t.ex. för att fullgöra ett avtal mellan den personuppgiftsansvarige och den registrerade, eller om det i annat fall är tillåtet enligt föreskrifter av regeringen eller Datainspektionen som behövs med hänsyn till ett viktigt allmänt intresse eller om det finns tillräckliga garantier till skydd för de registrerades rättigheter. Sådana garantier har ställts bl.a. genom standardavtalsklausuler som EU-kommissionen godkänt (13 § första stycket 2 personuppgiftsförordningen).

Standardavtalsklausulerna är avtalsklausuler med skyldigheter för både personuppgiftsansvariga som vill överföra uppgifter till tredje land och personuppgiftsansvariga eller personuppgiftsbiträdena som tar emot uppgifterna. Klausulerna reglerar även andra frågor, t.ex. de registrerades rättigheter och hur tvister med anledning av avtalet ska lösas. Syftet med avtalsklausulerna är att ge tillräckliga garantier så att enskildas rättigheter skyddas vid överföring av personuppgifter till länder som inte har en adekvat skyddsnivå. Den 3 oktober 2017 har Irlands högsta domstol för övrigt på begäran av den irländska dataskyddsombudsmannen beslutat att inhämta ett förhandsavgörande från EU-domstolen huruvida kommissionens standardavtalsklausuler ger tillräckliga garantier för européers fri- och rättigheter vid överföring av personuppgifter till USA (mål nr 2016 No. 4809 P).

Oaktat möjligheten att överföra personuppgifter till ett tredje land enligt PUL måste en personuppgiftsansvarig, t.ex. en vårdgivare, i Sverige alltid följa alla de övriga krav som följer av PUL, t.ex. de grundläggande kraven för all

personuppgiftsbehandling (9 §) och reglerna om när sådan behandling över huvud taget är tillåten.

Som framhållits ingår i den personuppgiftsansvariges laglighetsprövning att bedöma huruvida behandlingen av personuppgifter är laglig (9 § PUL). Det innebär indirekt ett krav på att beakta tillämpliga sekretess- och tystnadspliktsbestämmelser.

Bestämmelser om sekretess och tystnadsplikt i den offentliga förvaltningen finns i huvudsak i offentlighets- och sekretesslagen (2009:400; OSL). Bestämmelser om tystnadsplikt hos privata rättssubjekt regleras normalt i annan lagstiftning.

Sekretess definieras enligt OSL som ett förbud att röja en uppgift, vare sig det sker muntligen, genom utlämnande av en allmän handling eller på något annat sätt (3 kap. 1 §). En bestämmelse om sekretess medför således både tystnadsplikt för de personer som har en skyldighet att följa bestämmelsen och handlings-sekretess för de handlingar som omfattas av bestämmelsen.

När det gäller sekretessens styrka är det normala att den bestäms med hjälp av s.k. skaderekvisit. Man skiljer i detta avseende mellan rakt och omvänt skaderekvisit. Vid rakt skaderekvisit är utgångspunkten att uppgifterna är offentliga och att sekretess endast gäller om det kan antas att viss skada uppstår om uppgifterna lämnas ut. Vid omvänt skaderekvisit är utgångspunkten den motsatta, dvs. att uppgifterna omfattas av sekretess. Vid omvänt skaderekvisit får uppgifterna således bara lämnas ut om det står klart att detta kan ske utan att viss skada uppstår. Sekretessen enligt en bestämmelse kan även vara absolut, vilket innebär att de uppgifter som omfattas av bestämmelsen ska hemlighållas utan någon skadeprövning.

Bestämmelser om sekretess och tystnadsplikt ska inte bara iakttas av myndighet när uppgifter begärs utlämnade av enskilda utan även när en myndighet, t.ex. en hälso- och sjukvårdsnämnd inom ett landsting, självmant eller på begäran av en annan vårdgivare överväger att lämna ut patientuppgifter.

Sekretess inom den offentliga hälso- och sjukvården finns reglerad i 25 kap. 1 § OSL. Sekretessen har ett omvänt skaderekvisit, dvs. utgångspunkten är att det råder sekretess för uppgifter om enskilds personliga förhållanden och hälsa. Ett utlämnande till enskild eller myndighet får därmed enbart ske med patientens medgivande, efter en skadeprövning (menprövning) eller med stöd av en sekretessbrytande bestämmelse.

Det finns inte utrymme i detta yttrande för att gå igenom alla sekretessbrytande bestämmelser som finns spridda i OSL och andra författningar, t.ex. patientsäkerhetslagen. Av intresse är 10 kap. 2 § OSL. Enligt bestämmelsen hindrar sekretess inte att en uppgift lämnas till en enskild eller till en annan myndighet, om det är nödvändigt för att den utlämnande myndigheten ska kunna fullgöra sin verksamhet. Syftet med bestämmelsen är att förhindra att sekretessregleringen gör det omöjligt för en myndighet och dess personal att sköta sina uppgifter, dvs. att fullgöra det uppdrag som följer av myndighetens instruktion, andra författningar, regleringsbrevet och särskilda regeringsbeslut. I förarbetena nämns flera exempel på situationer när bestämmelsen aktualiseras (prop. 1979/80:2 Del A s. 121).

Även om bestämmelsen ska tillämpas restriktivt är avsikten inte att den ska tillämpas endast i situationer av undantagskaraktär. Både E-delegationen och eSam anser efter en utförlig genomgång av förarbeten och praxis att tillgängliggörande av uppgifter i samband med sådan outsourcing som sker i syfte att dra nytta av utförarens expertkompetens eller tekniska utrustning i särskilda fall bör anses utgöra ett nödvändigt utlämnande som bryter sekretess (se E-delegationen, Sekretess vid outsourcing – en förstudie, Fi 2009:01/2015/4 respektive eSam, Outsourcing – en vägledning om sekretess och persondataskydd). I det s.k. Conscriptorbeslutet har emellertid JO givit uttryck

för en mer restriktiv syn på tillämpningsområdet för 10:2 OSL (beslut 9 september 2014). Rättsläget är således oklart för 10:2 OSL.

Av betydelse vid röjande av sekretessbelagda uppgifter med stöd av en sekretessbrytande bestämmelse är att uppgifterna alltjämt har ett godtagbart skydd hos mottagaren. Om mottagaren är en myndighet kan sekretess råda för uppgifterna hos den myndigheten. Om mottagaren är en privat aktör, t.ex. en expert eller en leverantör av digitala tjänster som myndighet anlitar, är det inte självklart att dessa omfattas av en lagstadgad tystnadsplikt. Lagstiftaren har i vissa fall sett till att auktoriserade tolkar och chaufförer som bedriver färdtjänst omfattas av en lagstadgad tystnadsplikt (se förordning [1985:613] om auktorisation av tolkar och översättare samt lagen [1997:736] om färdtjänst). Företag som levererar digitala tjänster åt myndigheter omfattas däremot inte av en lagstadgad tystnadsplikt. (Det fanns emellertid en sådan lagstadgad tystnadsplikt för leverantörer i den äldre datalagen, 13 §, men den fördes inte över till PUL av okänd anledning.)

l förarbetena till den numera upphävda sekretesslagen förordas för en sådan situation, nämligen då en ”skrivbyrå” anlitas för utskrift av handlingar som innehåller sekretessbelagda uppgifter, att myndigheter ställer krav på att det utförande företaget ska sluta avtal om tystnadsplikt med sin personal.[3] Huruvida ett sådant krav är tillräckligt för att en myndighet ska kunna lämna ut sekretessbelagda uppgifter i samband med outsourcing råder det delade meningar om. Förvisso kan en sådan mottagare inte åtalas för brott mot tystnadsplikt (20 kap. 3 § brottsbalken) eftersom tystnadsplikten enbart är avtalsreglerad och inte lagstadgad, men det utesluter inte att andra brott kan aktualiseras, t.ex. brotten dataintrång eller trolöshet mot huvudman (se E-delegationen, Sekretess vid outsourcing – en förstudie), vilket skulle tala för att avtalsreglerad tystnadsplikt ger samma skydd som en lagstadgad tystnadsplikt. Sammanfattningsvis finns enligt regionstyrelsens mening en påtaglig otydlighet i lagstiftningen i vilken utsträckning en avtalsreglerad tystnadsplikt är tillräcklig för att skydda sekretessbelagda uppgifter som lämnas ut till en privat tjänsteleverantör.

Frågan har fått ny aktualitet genom den nya dataskyddsförordningen. Datainspektionen har i en skrivelse till Justitiedepartementet den 7 juli 2017 (Datainspektionens dnr 1704-2017) bl.a. angett att det skyndsamt bör utredas huruvida den omfattande behandling av personuppgifter som sker inom bl.a. hälso- och sjukvården, genom outsourcing, är förenlig med art. 9.2 h och 9.3 i dataskyddsförordningen eller om det behöver införas en lagstadgad tystnadsplikt för de personuppgiftsbiträden som i dag inte omfattas av en sådan.

Om tveksamhet råder huruvida en överlåtelse av arbetsuppgifter som innefattar sekretessbelagda uppgifter till en privat tjänsteleverantör, t.ex. med stöd av 10 kap. 2 § OSL, får samma skydd hos leverantören med ett avtal om tystnadsplikt, står ett annat alternativ till buds – sekretessförbehåll. Bestämmelsen finns i 10 kap. 14 § OSL. Denna sekretessbrytande bestämmelse möjliggör för myndigheter att i förhållande till en privat aktör lämna ut uppgifter som är sekretessbelagda enligt en sekretessbestämmelse som har ett skaderekvisit. Utlämnande kan ske under förutsättning att den risk för skada, men eller annan olägenhet som hindrar att uppgifterna lämnas till den enskilde kan undanröjas genom att uppställa ett förbehåll. Det sagda innebär att uppgifter som omfattas av absolut sekretess inte kan lämnas ut med förbehåll. Ett förbehåll kan t.ex. avse ett förbud mot att lämna uppgifterna vidare eller utnyttja dem. Den tystnadsplikt

[3] Prop. 1981/82:186 s. 41–42.

som uppkommer genom förbehållet inskränker i vissa fall rätten att meddela och offentliggöra uppgifterna (meddelarfrihet).

Fördelen med sekretessförbehåll är att mottagarens röjande av uppgifterna kan medföra straffansvar för brott mot tystnadsplikten. Det finns emellertid begränsningar kring hur och när ett förbehåll får utfärdas. För det första får ett förbehåll inte meddelas i förväg utan ska föregås av en prövning i varje särskilt fall och avse en konkret mängd uppgifter. För det andra ska ett förbehåll meddelas som ett formligt beslut, dvs. det ska dokumenteras. För det tredje ska själva uppgiftsutlämnandet ske till en utpekad fysisk person. Det går inte enligt de uttalanden som gjorts om bestämmelsen (se t.ex. JK 2001-03-21, dnr 1719-99-22) att i avtal reglera generella förbehåll. Förbehållslösningen verkar bara fungera i sådana situationer där leverantören inte har behov av åtkomst till myndighetens information annat än i undantagsfall. Bestämmelsen om sekretessförbehåll har alltså inte anpassats för den senaste tidens digitalisering med upprepade behov av automatiserade ADB-utlämnanden till en mottagare som är en juridisk person, eller för den delen direktåtkomst. Det går inte då att i varje enskilt fall fatta ett beslut om sekretessförbehåll.

Yttrande

Såvitt regionstyrelsen förstår avser anmälningarna till JO det datautlämnande som skedde i april 2016 till BWPO och som uppmärksammades av Hallandsposten i ett flertal artiklar i oktober 2017. Anmälningarna korrelerar tidsmässigt med dessa artiklar.

Anmälarna har bl.a. ifrågasatt om utlämnandet av ”journalhandlingar” var lagligt, om berörda patienter informerats och om det funnits risker för anmälarnas fri- och rättigheter. Anmälarna menar att det inte har funnits några sekretessavtal eller sekretessförbindelser mellan Region Halland och BWPO.

Som framgår av redogörelsen för datautlämningen stämmer det att utlämnandet inte uppfyllde i alla delar författningsenliga krav på persondataskydd. Eftersom mottagarlandet USA saknar ett adekvat skydd för personuppgifter, och BWPO för övrigt inte omfattades av Kommissionens genomförandebeslut den 12 juli 2016 om adekvat skydd som säkerställs genom skölden för skydd av privatlivet i EU och Förenta staterna (EU-US Privacy Shield), skulle EU-kommissionens standardklausuler ha tecknats före överföringen, närmare bestämt standardavtalsklausulerna för personuppgiftsbiträden (2002/16/EC).

Region Halland har förvisso ingått ett samarbetsavtal med BWPO, men det samarbetet har förutsatt enligt regionstyrelsens beslut att BWPO ska ”Utveckla metoder för att analysera den data som redan finns i Region Halland” (se ovan). I dessa delar är BWPO i PUL:s mening anlitad av Region Halland i rollen som expert på dataanalyser och vårdflöden och behandlar således uppgifterna för regionens räkning på uppdragsbasis, dvs i rollen som personuppgiftsbiträde. Att BWPO i andra delar av samarbetet har en mer självständig ställning förändrar inte det förhållandet att organisationen ska ses som en utförare av dataanalyser åt Region Halland.

Det stämmer emellertid inte såsom anmälarna påstår att det inte fanns några avtal om tystnadsplikt mellan parterna. Av samarbetsavtalet mellan Region Halland och BWPO (punkten 4.5) framgår att parterna är eniga om att all information inom ramen för samarbetet ska betraktas som konfidentiell information, vilken information inte får röjas för obehörig part. Samtidigt erkänner BWPO Region Hallands skyldighet att iaktta offentlighetsprincipen. Tystnadsplikten är på en organisatorisk nivå utan några som helst förpliktelser eller sanktioner för BWPO:s medarbetare. Givetvis skulle regionstyrelsen kunnat ha övervägt en individuell avtalad tystnadsplikt vid tillfället med varje medarbetare vid BWPO, men faktum är att BWPO har gett garantier om att iaktta sekretess för uppgifter som regionen röjer för BWPO.

Det stämmer inte att Region Halland lämnade ut ”journalhandlingar”. Det var ett begränsat antal specifika uppgifter ur patientjournaler och andra vårdadministrativa system som lämnades ut. Uppgifterna innehöll inte några uppgifter som direkt kunde hänföras till enskilda patienter hos mottagaren. Några namn eller personnummer lämnades således inte ut.

Med facit på hand kan konstateras dock att det vid utlämnandetillfället rörde sig om personuppgifter i PUL:s mening, dock i pseudonymiserad form. Berörda medarbetare och chefer inom regionkontoret ansåg dock att det var fråga om helt avidentifierade uppgifter på vilka PUL och patientdatalagen inte var tillämpliga. Det betyder dock inte att regionkontoret negligerade persondataskyddet. Pseudonymisering betraktas som en godtagbar kompensatorisk mekanism för att minska risken för enskildas fri- och rättigheter vid personuppgiftsbehandling. I dataskyddsförordningen finns flera artiklar och skäl som upptar uttryckligen pseudonymisering som en effektiv metod för att skydda enskildas personliga integritet, t.ex. art. 25.1 (inbyggt dataskydd).

BWPO har vidare efter genomförda analyser av utlämnade data utplånat desamma, vilket organisationen intygat skriftligen. Konverteringsfilen innehållande löpnummer för varje patients data som lämnades ut, och namn och personnummer i regionens eget datalager, är också utplånad.

Beträffande den lagliga grunden för utlämnandebehandlingen så äger Region Halland i rollen som sjukvårdshuvudman och vårdgivare laglig rätt med stöd av PDL att behandla patientuppgifter utan registrerades samtycke för bl.a. uppföljning, utveckling och kvalitetssäkring av hälso- och sjukvården som bedrivs i länet, förutsatt att behandlingen är nödvändig. Information om regionens personuppgiftsbehandling förmedlas på olika sätt, bl.a. genom regionens hemsida och anslag i väntrum. Region Hallands utnyttjande i detta fall av ett personuppgiftsbiträde (BWPO) ställer inga särskilda krav på information till de registrerade utöver den informationsplikt som framgår av PDL. Utlämnandebehandlingen har således skett som ett led i Region Hallands behandling av personuppgifter för de ändamål som anges i 2 kap. 4 § PDL och har ansetts nödvändig för regionens utvecklingsarbete (Framtidsarbete) och hälso- och sjukvårdsstrategi.

Beslutet om att lämna ut uppgifterna har fattats i laga ordning, däremot kan det i efterhand konstateras att delegatens beslut och skäl för beslutet borde ha dokumenterats tydligare än vad som är fallet. Å ena sidan ställs inga författningsenliga krav på dokumentation av ett beslut om utlämnande av uppgifter som omfattas av sekretess. Å andra sidan får det anses viktigt för rättssäkerheten och allmänhetens insyn i den offentliga förvaltningen att större uppgiftsutlämnanden, s.k. massuttag (prop. 1979/80:2 Del A s. 81 f.), som innefattar såpass känsliga uppgifter som uppgifter om enskildas hälsa dokumenteras på lämpligt sätt av ansvarig tjänsteman eller nämnd.

Regionstyrelsens uppfattning är att det inte funnits någon risk alls för enskildas fri- och rättigheter, bl.a. rörande skyddet för privatlivet, genom det utlämnande av data som skedde i april 2016 till BWPO och rådande avtalad tystnadsplikt. Detta varken vid överföringen över internet eller vid BWPO:s databehandling av uppgifterna. BWPO har inte haft en möjlighet att bakåtidentifiera enskilda individer. Regionstyrelsen baserar den uppfattningen bl.a. på de åtgärder som vidtogs vid överföringen av uppgifterna, bl.a. pseudonymiseringen av personuppgifterna.

Det bör också i sammanhanget uppmärksammas att BWPO själva driver en välrenommerad hälso- och sjukvårdsverksamhet, och är därför väl förtrogna med de krav som ställs inom hälso- och sjukvården på konfidentialitet för patientuppgifter, liksom att tystnadsplikten utgör en viktig del av en god och säker hälso- och sjukvård. BWPO har också givit skriftliga garantier att uppgifterna är utplånade.

> Med anledning av den förda diskussionen rörande samarbetet mellan Region Halland och BWPO har regionstyrelsen under 2017 bland annat genomfört en juridisk analys avseende persondataskyddet i samarbetet med BWPO. Något utlämnande av det slag som skedde i april 2016 har dessutom inte förekommit sedan dess, och som beskrivits var syftet med utlämnandet att lägga grunden till SHARP. BWPO:s arbete sker under strikt kontrollerade former och enbart på plats i Region Hallands egna lokaler och egen data- och analysmiljö.

AA och BB gavs tillfälle att kommentera remissvaret.

JO hämtade därefter in och granskade i valda delar det aktuella samarbetsavtalet mellan regionen och Brigham and Women's Physicians Organization Inc. (BWPO).

Bedömning

Allmänna utgångspunkter

Av utredningen får bl.a. följande anses utrett. Region Halland tecknade den 2 februari 2016 ett samarbetsavtal med BWPO, med säte i USA, gällande forskning och utveckling. I avtalet fanns en klausul om att all information inom ramen för samarbetet var konfidentiell och inte fick röjas för någon obehörig part. Det tecknades dock inte några avtal om individuell tystnadsplikt för BWPO:s medarbetare. Ett syfte med samarbetet var att utveckla metoder för att analysera de data som redan fanns inom regionens hälso- och sjukvård. Som ett led i detta lämnade regionen i april 2016 ut uppgifter ur patientjournaler – bl.a. diagnoser, labbsvar, läkemedelsanvändning och födelseår – till BWPO. Uppgifterna lämnades ut utan patienternas namn och personnummer, men med angivande av ett löpnummer för varje patient. Patienternas personnummer och löpnummer bevarades i en separat referensfil som inte lämnandes ut till BWPO. De aktuella uppgifterna fördes över till BWPO i en krypterad fil över internet på en krypterad förbindelse. Såvitt framkommit har såväl de data som lämnades ut till BWPO som referensfilen numera utplånats.

Uppgifter ur patientjournaler är typiskt sett information som är mycket känslig ur integritetssynpunkt. Inom hälso- och sjukvården skyddas sådana uppgifter genom dels bestämmelser om hur personuppgifter får behandlas, dels bestämmelser om sekretess och tystnadsplikt. Utgångspunkten är att sekretess gäller för sådana uppgifter.

Regler om behandling av personuppgifter inom hälso- och sjukvården fanns – vid den tidpunkt då data lämnades ut till BWPO – framför allt i patientdatalagen (2008:355) och personuppgiftslagen (1998:204). Personuppgiftslagen upphävdes den 25 maj 2018 när Dataskyddsförordningen (GDPR, The General Data Protection Regulation) trädde i kraft. I samband med det ändrades även vissa bestämmelser i patientdatalagen. Nedan hänvisas till de bestämmelser i personuppgiftslagen och patientdatalagen som gällde i april 2016 om inte annat anges.

De båda ärendena aktualiserar ett flertal komplexa integritetsfrågor. Jag har dock inte haft möjlighet att fördjupa mig i samtliga dessa frågor inom ramen för

denna utredning. Min granskning kommer därför främst att rikta in sig på frågorna om det aktuella utlämnandet av uppgifter var förenligt med dels reglerna om behandling av personuppgifter, dels sekretesslagstiftningen. Jag kommer även att kort beröra frågan om dokumentation.

I sammanhanget vill jag även framhålla att utvecklingsarbete som utförs på vetenskaplig grund och innefattar behandling av känsliga personuppgifter kräver etikgodkännande (se vidare lagen [2003:460] om etikprövning av forskning som avser människor). Jag har i min granskning valt att inte närmare undersöka syftet med det aktuella samarbetet mellan regionen och BWPO utan utgått från att det enbart har innefattat annat kvalitets- och utvecklingsarbete på det sätt som regionen har angett. Vid min bedömning har jag vidare utgått från att BWPO i förhållande till regionen agerar i egenskap av personuppgiftsbiträde och behandlar personuppgifter för den personuppgiftsansvariges (dvs. regionens) räkning (jfr 3 § personuppgiftslagen).

Rättslig reglering m.m.

Regler om hantering av personuppgifter inom hälso- och sjukvården

Patientdatalagen innehåller särskilda regler om behandling av personuppgifter inom hälso- och sjukvården, medan det i personuppgiftslagen fanns allmänna regler om behandling av personuppgifter. Den dåvarande regleringen innebar att personuppgiftslagen skulle tillämpas om frågan inte var reglerad i patientdatalagen eller i en annan lag eller förordning (se 2 § personuppgiftslagen och 1 kap. 4 § patientdatalagen).

Med personuppgift avses all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet (3 § personuppgiftslagen). Även krypterade uppgifter omfattas av lagen så länge någon kan göra uppgifterna läsbara och därmed identifiera individer (se bl.a. SOU 1997:39 s. 341). Också sådana i sig anonyma uppgifter som gör det möjligt att utföra en s.k. bakvägsidentifikation av en fysisk person omfattas. Det krävs bara att en fysisk person kan identifieras med hjälp av uppgifterna, inte att den personuppgiftsansvarige själv ska förfoga över samtliga uppgifter som gör identifieringen möjlig.

Personuppgifter får behandlas inom hälso- och sjukvården om det behövs bl.a. för att systematiskt och fortlöpande utveckla och säkra kvaliteten i verksamheten samt för administration, planering, uppföljning, utvärdering och tillsyn av verksamheten (2 kap. 4 § första stycket 3 och 4 patientdatalagen).

Det är vårdgivaren som är personuppgiftsansvarig för den behandling av personuppgifter som vårdgivaren utför (2 kap. 6 § patientdatalagen). Den personuppgiftsansvarige skulle bl.a. se till att personuppgifter bara behandlades om det var lagligt samt på ett korrekt sätt och i enlighet med god sed (9 § första stycket a och b personuppgiftslagen).

Vårdgivare måste även bl.a. beakta Socialstyrelsens föreskrifter (t.ex. SOSFS 2008:14 om informationshantering och journalföring i hälso- och sjukvården,

den 1 mars 2017 ersatt av HSLF-FS 2016:40 om journalföring och behandling av personuppgifter i hälso- och sjukvården).

Överföring av personuppgifter till tredje land

I patientdatalagen saknas bestämmelser om överföring av personuppgifter till tredje land. I personuppgiftslagen reglerades frågan i 33–35 §§. Huvudregeln var att tredjelandsöverföring var förbjuden till länder som inte hade en adekvat nivå för skyddet av personuppgifter (33 §). Frågan om huruvida en skyddsnivå var adekvat skulle bedömas med hänsyn till samtliga omständigheter som hade samband med överföringen. Särskild vikt skulle läggas vid uppgifternas art, ändamålet med behandlingen, hur länge behandlingen skulle pågå, ursprungslandet, det slutliga bestämmandelandet och de regler som fanns för behandlingen i det tredje landet. Med tredje land avses en stat som inte ingår i EU eller är ansluten till EES (3 § personuppgiftslagen).

Regeringen kunde meddela föreskrifter om generella undantag från förbudet (35 §). Överföring kunde vara tillåtet till exempelvis bolag i USA som var anslutna till de s.k. Safe Harbor-principerna eller om parterna använde sig av EU-kommissionens standardavtalsklausuler (se vidare 13 § personuppgifts-förordningen [1998:1191] och bilaga 1–2 till förordningen).

Regler om sekretess m.m. inom den allmänna hälso- och sjukvården

Inom hälso- och sjukvården gäller sekretess för en uppgift om en enskilds hälsotillstånd eller andra personliga förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till honom eller henne lider men (25 kap. 1 § offentlighets- och sekretesslagen [2009:400], OSL). Det innebär att det råder presumtion för sekretess och i vilka fall uppgifter kan lämnas ut måste avgöras efter en skadeprövning från fall till fall (se Lenberg m.fl., Offentlighets- och sekretesslagen [9 januari 2019, Zeteo], kommentaren till 25 kap. 1 §).

Sekretess gällde även tidigare för personuppgift, om det kunde antas att ett utlämnande skulle medföra att uppgiften behandlades i strid med person-uppgiftslagen (21 kap. 7 § OSL i dess lydelse före den 25 maj 2018).

En uppgift för vilken sekretess gäller enligt OSL får inte röjas för enskilda eller för andra myndigheter, om inte annat anges i OSL eller i lag eller förordning som OSL hänvisar till (8 kap. 1 § OSL). Det är förbjudet för såväl myndigheter som vissa personer (som har tystnadsplikt) att röja uppgifter som är sekretess-belagda (2 kap. 1 § OSL). Förbudet gäller för personer som har fått kännedom om uppgiften genom att för det allmännas räkning delta i en myndighets verksamhet på grund av anställning eller uppdrag hos myndigheten, på grund av tjänsteplikt, eller på annan liknande grund (2 kap. 1 § andra stycket OSL). Bestämmelsen gäller i princip inte den som är anställd hos ett privat rättssubjekt (se prop. 1979/80:2 Del A s. 128). JO har tidigare uttalat att personalen hos ett personuppgiftsbiträde som journalförde patientuppgifter inte omfattades av

någon straffsanktionerad tystnadsplikt som följer av 2 kap. 1 § andra stycket OSL (se JO 2015/16 s. 606).

Ett flertal sekretessbrytande bestämmelser finns i OSL. Sekretess hindrar som regel inte att en uppgift lämnas till en annan enskild eller till en myndighet om den enskilde samtycker till det (10 kap. 1 § och 12 kap. OSL). Sekretess hindrar inte heller att en uppgift lämnas till en enskild eller till en annan myndighet, om det är nödvändigt för att den utlämnande myndigheten ska kunna fullgöra sin verksamhet (10 kap. 2 § OSL). Av förarbetena framgår att bestämmelsen i 10 kap. 2 § OSL ska tillämpas restriktivt, och det räcker t.ex. inte att myndighetens verksamhet blir mindre effektiv om uppgiften inte lämnas ut (a. prop. s. 465 och 494). JO har i flera ärenden resonerat om bestämmelsens räckvidd och ansett att det handlar om situationer av undantagskaraktär (se bl.a. JO 2015/16 s. 606).

En sekretessbelagd uppgift kan i vissa fall även lämnas ut om myndigheten ställer upp ett förbehåll som inskränker den enskildes rätt att lämna uppgiften vidare eller utnyttja den (10 kap. 14 § OSL). Ett sådant förbehåll ska dock ställas upp i förhållande till en enskild mottagare, föregås av en prövning i varje enskilt fall och avse en konkret mängd uppgifter (se bl.a. JO 1992/93 s. 197 och 1994/95 s. 574).

Ett röjande av en uppgift kan ske muntligen, genom utlämnande av en allmän handling eller på något annat sätt (3 kap. 1 § OSL). Den som omfattas av tystnadsplikt och felaktigt röjer en uppgift kan i vissa fall dömas för brott mot tystnadsplikten (20 kap. 3 § brottsbalken).

Bedömningen i det aktuella fallet

Utlämnandets förenlighet med reglerna om överföring av personuppgifter till tredje land

Utifrån de omständigheter som framgår av remissvaret har jag inte några principiella synpunkter på att regionen har ansett det nödvändigt att behandla personuppgifter i sitt arbete med kvalitetssäkring av verksamheten (jfr 2 kap. 4 § patientdatalagen). Vidare delar jag regionens uppfattning att användandet av ett personuppgiftsbiträde i sig inte medförde några särskilda krav på information till patienterna.

När det gäller de data som lämnades ut till BWPO kan jag konstatera att uppgifterna inte var helt avidentifierade eftersom det med hjälp av referensfilen fortfarande var möjligt att identifiera enskilda individer. Uppgifterna var därmed att anse som personuppgifter, även om de lämnades ut i pseudonymiserad form. Jag noterar att regionen vid utlämnandet av uppgifterna således hade en felaktig uppfattning i den frågan.

Såvitt har framkommit i ärendena saknade mottagarlandet USA vid utlämnandet av uppgifterna ett adekvat skydd för personuppgifter, BWPO var inte ansluten till de s.k. Safe Harbor-principerna och parterna hade inte heller tecknat EU-

kommissionens standardavtalsklausuler. Mot den bakgrunden delar jag regionens bedömning att utlämnandet inte var förenligt med då gällande lagstiftning om behandling av personuppgifter. För detta förtjänar regionen kritik.

Utlämnandets förenlighet med sekretesslagstiftningen

Som framgått ovan är huvudregeln inom hälso- och sjukvården att sekretess råder för uppgifter i t.ex. en patientjournal. Utifrån den information som jag har tagit del av kan BWPO:s medarbetare inte anses omfattas av bestämmelserna om tystnadsplikt i 2 kap. 1 § OSL (jfr bl.a. JO 2015/16 s. 606). Sekretess enligt 25 kap. 1 § OSL gällde alltså i förhållande till BWPO och dess medarbetare.

Vid utlämnandet hade de aktuella journaluppgifterna pseudonymiserats, och BWPO fick inte tillgång till den referensfil som innehöll patienternas löpnummer och personnummer. I förarbetena till den tidigare sekretesslagen (1980:100) anges bl.a. följande (se prop. 1979/80:2 Del A s. 84):

> För att enskild person ska lida skada eller men krävs givetvis att uppgifterna är hänförliga till en viss individ. Det innebär att man i allmänhet bör kunna lämna ut s.k. avidentifierade uppgifter utan att risk för skada eller men uppkommer. I enstaka fall kan det emellertid tänkas att en avidentifiering inte är tillräcklig för att hindra att sambandet mellan individen och uppgiften spåras. Huruvida en sådan risk föreligger får givetvis bedömas efter omständigheterna i det enskilda fallet.

Begreppet ”avidentifierade uppgifter” definieras såvitt jag har kunnat se inte i den ovan angivna propositionen. Jag vill därför framhålla att tillämpningen av begreppet under senare år har blivit mer restriktiv och att det som avsågs i förarbetena till den tidigare sekretesslagen torde ha varit det som i dag kallas pseudonymiserade uppgifter, dvs. information utan direktidentifierande uppgifter (jfr definitionen i artikel 4 punkten 5, GDPR).

Att lämna ut uppgifter i pseudonymiserad form kan alltså medföra att det saknas risk för att en enskild person ska lida skada eller men, och att uppgifterna då kan lämnas ut. Det är emellertid viktigt att den utlämnande myndigheten gör en noggrann prövning av vilka uppgifter som kan lämnas ut, och hur utlämnandet bör ske, för att inte riskera att röja enskilda individer. Vid bedömningen anser jag att myndigheten bör beakta bl.a. vilken typ av uppgifter som omfattas, vem som är mottagare, vilken spridning uppgifterna kommer att få, hur uppgifterna kommer att hanteras av mottagaren, vilka som har tillgång till referensuppgifterna och vilka risker som finns för ytterligare spridning av uppgifterna.

I det här fallet anser jag att det finns flera omständigheter som borde ha manat till försiktighet. Utlämnandet har omfattat ett stort antal olika variabler, bl.a. uppgifter om diagnos, läkemedelsanvändning, vårdgivare, födelseår och bosättningskommun. Det rör sig enligt min mening om uppgifter som dels är av mycket integritetskänsligt slag, dels rent generellt kan underlätta identifiering av enskilda individer. Utredningen har inte gett svar på hur många medarbetare hos BWPO som hade tillgång till de aktuella personuppgifterna. Jag kan dock

konstatera att dessa personer såvitt kommit fram i ärendena inte omfattades av någon individuell tystnadsplikt, vare sig lagreglerad eller avtalad, i förhållande till dessa uppgifter. Vidare tycks den aktuella referensfilen ha varit en elektronisk fil som ett flertal medarbetare inom regionen hade teknisk tillgång till i sina datorer. Jag noterar att det enligt remissvaret har rört sig om i vart fall åtta medarbetare, varav tre konsulter.

Det har genom utredningen inte gått att klarlägga i vilken utsträckning det i detta fall var möjligt att trots pseudonymiseringen identifiera enskilda individer utifrån de uppgifter som lämnades ut. Såväl de utlämnade uppgifterna som referensfilen är enligt uppgift i remissvaret numera utplånade. Det framstår dock enligt min mening inte som osannolikt att s.k. bakvägsidentifiering i vissa fall skulle ha varit möjlig. Det framgår inte av regionstyrelsens remissvar att utlämnandet föregåtts av någon egentlig prövning av risken för att enskilda skulle lida men. Jag är kritisk till hanteringen och vill erinra om vikten av att en myndighet även vid utlämnande av personuppgifter i pseudonymiserad form gör en noggrann sekretessprövning utifrån omständigheterna i varje enskilt fall.

Särskilt om tillämpningen av 10 kap. 2 § OSL och avtalsreglerad tystnadsplikt

Regionstyrelsen har i sitt remissvar anfört att rättsläget är oklart vad gäller tillämpningen av bestämmelsen i 10 kap. 2 § OSL om nödvändigt utlämnande för att kunna fullgöra myndighetens verksamhet samt att det finns en otydlighet i fråga om i vilken utsträckning en avtalsreglerad tystnadsplikt är tillräcklig för att skydda sekretessbelagda uppgifter som lämnas ut till en privat tjänste-leverantör.

Som framgått av redogörelsen för den rättsliga regleringen ovan har såväl förarbetsuttalanden som uttalanden från JO förespråkat en restriktiv tillämpning av bestämmelsen i 10 kap. 2 § OSL. Jag är medveten om att det finns andra uppfattningar (se t.ex. Outsourcing – en vägledning om sekretess och persondataskydd, eSam, januari 2016 s. 27 f.) och att det finns ett behov av ytterligare vägledning i dessa frågor. De frågor som regionstyrelsen lyfter fram har behandlats i offentliga utredningar, bl.a. i betänkandet Juridiken som stöd för förvaltningens digitalisering (SOU 2018:25). Där föreslås bl.a. en straffsanktionerad tystnadsplikt för privata leverantörer när myndigheter har utkontrakterat it-drift eller andra it-baserade funktioner. Jag har i mitt yttrande över betänkandet ställt mig positiv till det förslaget (se mitt yttrande den 20 september 2018, dnr R 53-2018).

Mot den redovisade bakgrunden finner jag för närvarande inte anledning att göra några uttalanden i dessa frågor. Jag kommer dock att fortsätta följa utvecklingen på området.

Frågan om dokumentation

Avslutningsvis kan jag konstatera att det av remissvaret framgår att det finns brister i regionens dokumentation i det aktuella ärendet, t.ex. vad gäller skälen för beslutet att lämna ut personuppgifter till BWPO. Jag vill därför framhålla att

jag anser det mycket angeläget att viktiga åtgärder i myndigheters verksamhet dokumenteras på lämpligt sätt, bl.a. för att garantera allmänhetens insyn och möjliggöra en kontroll av handläggningen i efterhand. Det gäller i synnerhet när åtgärderna som i detta fall innefattar hantering av mycket integritetskänsliga uppgifter där det finns ett befogat intresse av insyn och granskning, såväl från enskilda som från andra externa kontrollfunktioner. Regionen kan mot den bakgrunden inte undgå kritik för sin bristande dokumentation.

Övrigt

Vad som i övrigt har kommit fram i ärendena föranleder inte några uttalanden från min sida.

Jag anser att det finns anledning att skicka beslutet till Datainspektionen och Socialdepartementet för kännedom.

Ärendena avslutas.