

Allvarlig kritik mot vissa vårdgivare inom dels Västra Götalandsregionen, dels Stockholms läns landsting för att man har ingått avtal om journalföring med ett företag trots att detta inte varit förenligt med regelverket om sekretess inom hälso- och sjukvården

Beslutet i korthet: Vårdgivare inom Västra Götalandsregionen och Stockholms läns landsting har ingått avtal med ett företag om hjälp med journalföring av patientuppgifter. Enligt avtalen agerar företaget som ett personuppgiftsbiträde i förhållande till vårdgivaren (som är personuppgiftsansvarig). Avtalen innebär att vårdgivaren tillåter att läkarsekreterare som är anställda hos företaget på distans lyssnar av inlästa diktat och skriver in uppgifterna i patientens journal. Hanteringen är helt elektronisk och uppgifter lagras aldrig utanför landstingets/regionens it-system.

Enligt 25 kap. 1 § offentlighets- och sekretesslagen (2009:400), OSL, råder en stark sekretess till skydd för uppgifter om patienter inom den allmänna hälso- och sjukvården. Reglerna om behandling av personuppgifter inom hälso- och sjukvården har inte någon direkt betydelse för hur sekretessfrågan ska prövas; frågan om en vårdgivare kan lämna ut sekretessbelagda uppgifter till ett personuppgiftsbiträde eller till personal hos biträdet ska prövas på vanligt sätt enligt OSL.

JO konstaterar att läkarsekreterarna hos företaget inte omfattas av den tystnadsplikt enligt OSL som gäller för vårdgivarens egen personal. Frågan om huruvida uppgifterna i patientjournalerna kan göras tillgängliga för läkarsekreterarna är därför i första hand beroende av om ett utlämnande kan ske utan att det innebär men (dvs. skada) för den som skyddas av sekretessen.

Läkarsekreterarna har en avtalsreglerad tystnadsplikt i förhållande till arbetsgivaren (dvs. företaget). Vidare följer av regelverket om behandling av personuppgifter en sorts tystnadsplikt för den som behandlar uppgifterna. Enligt JO är dessa "alternativa" tystnadsplikter för läkarsekreterarna inte tillräckliga för att anse att ett utlämnande kan ske utan att det innebär men (skada) för den som skyddas av sekretessen. Vid bedömningen har – mot bakgrund av att de uppgifter som behandlas enligt avtalen är av mycket integritetskänsligt slag – vikt lagts bl.a. vid att vårdgivarens egen personal kan dömas för brott mot tystnadsplikt om en sekretessbelagd uppgift felaktigt röjs, medan så inte är fallet när det gäller läkarsekreterare som är anställda i företaget. Ett utlämnande har inte heller haft stöd i någon av de sekretessbrytande bestämmelser som finns i 10 kap. OSL eller i en lag eller förordning som OSL hänvisar till.

JO:s slutsats är att vårdgivarna inte har haft rättsligt stöd för att på det sätt som skett lämna ut sekretessbelagda uppgifter om patienter för journalföring av företagets läkarsekreterare. Enligt JO är det anmärkningsvärt att vårdgivarna inte har ägnat sekretess-

aspekterna större uppmärksamhet i samband med att avtalen ingicks. Vårdgivarna får allvarlig kritik för att de har ingått avtal som innebär att landstinget/regionen lämnar ut patientuppgifter för journalföring av anställda vid ett företag, trots att detta inte är förenligt med regelverket om sekretess.

Innehåll

1	Anmälan.....	3
2	Utredning	3
2.1	Yttrande från Primärvårdsstyrelsen i Västra Götalandsregionen	3
2.2	Yttrande från Styrelsen för Angereds Närsjukhus i Västra Götalandsregionen.....	5
2.3	Yttrande från Styrelsen för Stockholms läns sjukvårdsområde (SLSO) i Stockholms läns landsting.....	5
2.4	Yttrande från Socialstyrelsen	7
2.5	Yttrande från Datainspektionen.....	9
3	Bedömning.....	11
3.1	Inledning	11
3.2	Regler om sekretess och tystnadsplikt m.m.	13
3.2.1	Sekretess inom den allmänna hälso- och sjukvården m.m.	13
3.2.2	Bestämmelser om tystnadsplikt för personal inom hälso- och sjukvården m.m.	13
3.2.2.1	Straffsanktionerad tystnadsplikt	13
3.2.2.2	Tystnadsplikt för personal inom den enskilda hälso- och sjukvården	14
3.2.2.3	Tystnadsplikt för personal inom den allmänna hälso- och sjukvården	14
3.2.3	Gäller någon form av tystnadsplikt för personalen (läkarsekreterare) som utför journalföringen hos personuppgiftsbiträdet?.....	16
3.2.3.1	Avtalsreglerad tystnadsplikt	17
3.2.3.2	En form av tystnadsplikt följer av reglerna om behandling av personuppgifter.....	17
3.3	Sekretessbrytande bestämmelser i OSL	18
3.3.1	Den sekretessbrytande bestämmelsen om nödvändigt utlämnande i 10 kap. 2 § OSL.....	18
3.3.2	Den sekretessbrytande bestämmelsen om utlämnande med förbehåll i 10 kap. 14 § OSL.....	19
4	Sammanfattande synpunkter.....	20
4.1	Utgångspunkter	20
4.2	Har det funnits rättsliga förutsättningar för vårdgivarna att lämna ut patientuppgifter på det sätt som följer av avtalen?.....	20
4.3	Avslutande synpunkter.....	22
4.4	Övrigt	22

1 Anmälan

I en anmälan anförde AA bl.a. att JO borde granska om sekretessen för journalförda uppgifter om patienter upprätthålls när uppgifterna överförs till ett privat bolag, Conscriptor, för att därefter behandlas av bolagets anställda i deras bostäder. Han hänvisade till en artikel som hade varit publicerad i dagstidningen Bohusläningen den 3 juni 2011.

Av artikeln framgick bl.a. följande. Conscriptors affärsidé är att hjälpa till med hanteringen av patientjournaler när den ordinarie personalen inom sjukvården inte hinner med. Uppdrag utförs åt sjukhus och vårdcentraler i hela Sverige. Företaget har utvecklat en egen teknisk plattform och kan kommunicera med de olika system för databehandling som de olika vårdgivarna använder sig av. De flesta av företagets anställda arbetar på distans från den egna bostaden.

2 Utredning

I anmälan och tidningsartikeln nämndes vissa vårdinrättningar. JO hämtade in kopior av avtal mellan Conscriptor och Stockholms läns sjukvårdsområde (SLSO) inom Stockholms läns landsting samt mellan Conscriptor och Vårdcentralen i Hindås, Västra Götalandsregionen.

Därefter begärde JO att dels vederbörande nämnd inom Västra Götalandsregionen, dels Styrelsen för SLSO skulle yttra sig till JO. Yttrandena skulle – bl.a. mot bakgrund av den sekretess som gäller inom hälso- och sjukvården för uppgift om en enskilds hälsotillstånd eller andra personliga förhållanden (25 kap. 1 § offentlighets- och sekretesslagen [2009:400], OSL) – avse vilka överväganden som hade gjorts innan uppgifter om patienter hade överförts från landstinget/regionen till Conscriptor.

Av en skrivelse från Juridiska enheten vid Västra Götalandsregionens regionkansli framgick att Conscriptor hade anlitats av primärvården och Angered's Närsjukhus, samt att yttranden hade inhämtats från de nämnder som är ansvariga för dessa verksamheter.

2.1 Yttrande från Primärvårdsstyrelsen i Västra Götalandsregionen

I sitt yttrande anförde Primärvårdsstyrelsen bl.a. följande (omnämnda bilagor har utelämnats):

Utredning

Conscriptor AB är ett företag som tillhandahåller tjänster för digital journalhantering på distans till ett flertal vårdgivare i Sverige. Västra Götalandsregionen anlitar företaget genom en beställning som görs av respektive verksamhetschef. Behovet av att anlita en extern leverantör har uppkommit som en följd av kravet i primärvården på att diktat ska vara inskrivna i patientjournalen inom fem dagar, vilket man inte alltid har kunnat leva upp till med ordinarie personal.

När det är aktuellt att anlita Conscriptor träffas första gången ett lokalt avtal mellan verksamhetschefen och företaget, se exempel på avtal i bilaga 2. I detta tydliggörs att vårdgivaren är personuppgiftsansvarig och att Conscriptor agerar person-

uppgiftsbiträde. Conscriptor svarar för att behandlingen av personuppgifter sker enligt Personuppgiftslagen och enligt kundens instruktioner. Conscriptor ansvarar i sitt arbete som personuppgiftsbiträde för att vidta de säkerhetsåtgärder som avses i personuppgiftslagen 31 § första stycket samt i enlighet med kundens policy och riktlinjer för informationssäkerhet. Regionens information till personal bifogas, bilaga 3.

I avtalet anges att kunden har rätt att låta auktoriserad revisor eller annan av Conscriptor godkänd person granska Conscriptors hantering av kundens material i syfte att kontrollera att företaget uppfyller överenskomna säkerhetskrav. Primärvården har inte funnit anledning att göra detta.

Primärvården har granskat det avtal som används och har inte funnit något som visar på brister i förhållande till lagstiftningen eller regionens riktlinjer för informations-säkerhet.

Teknisk lösning

Conscriptors sekreterare kopplar upp sin dator till Västra Götalandsregionens nätverk via en säker förbindelse (VPN) med RSA-autentisering (inloggningsdosa) och med programvara som omöjliggör kommunikation med lokal utrustning inom Conscriptor. Inom regionens nätverk sker inloggning på en Citrixserver där ytterligare en inloggning sker till VGR:s journalsystem Medidoc eller Journal III. Programvaran för digital diktering – MedSpeech – plockar notat ur arbetslistan för att lyssna av diktaten samt skriva in dem i journalsystemet. Det finns spärrar som utesluter att ta skärmbilder för lagring på lokal dator och Citrixservern krypterar all trafik som sänds till/från Conscriptors dator.

Behörighet för inloggning till regionens nät sker via anmälan till fjärraccess och godkänns av IT-chef inom Primärvården. Behörighet för inloggning till journalsystem görs av verksamhetschef på vårdcentralen.

Regionen använder samma system och rutiner för egen personal som arbetar på äldreboende med skillnaden av att regionens personal använder SITHS-kort (tjänstekort) för autentisering istället för RSA-autentisering.

Bedömningen är att den tekniska lösningen har en mycket hög säkerhet ur ett IT-perspektiv.

Sammanfattande bedömning

Det faktum att Conscriptors läkarsekreterare i så stor omfattning utför arbetsuppgifterna i hemmet har inte varit känt för Primärvården innan JO-anmälan aktualiserade frågan.

När vi som vårdgivare utför denna typ av uppgifter i vår egen verksamhet sker det i lokaler där endast primärvårdens egen personal har tillträde. Detta innebär att samtliga omfattas av och är väl införstådda med reglerna för sekretess och den praktiska hanteringen av sekretessbelagd information. Vårdgivaren kan också kontrollera efterlevnaden.

När det gäller arbete som sker i hemmiljö kan primärvården, trots samma höga säkerhet i tekniska lösningar och personalens goda kunskap om hur sekretessbelagd information hanteras, aldrig kontrollera omgivningsfaktorerna, även om vi inte har anledning att betvivla att säkerheten är fullgod.

Slutsats

Primärvården Västra Götalandsregionen har förtroende för Conscriptor som leverantör av tjänst för journalhantering. Primärvården uppfattar att den tekniska säkerheten är mycket hög och att sekretessfrågorna är väl omhändertagna hos Conscriptor.

Eftersom Primärvården Västra Götalandsregionen inte kan kontrollera omgivningsfaktorer i hemmiljö är ställningstagandet att de uppgifter som tjänsten omfattar ska utföras i leverantörens lokaler. I Västra Götalandsregionens pågående upphandling av läkarsekreterartjänster är detta ett krav som är med i kravspecifikationen. Efter kontakt med regionens inköpsavdelning gavs besked om att nytt avtal bedöms vara klart under våren 2012.

Till yttrandet hade fogats kopior av dels ett ”journalhanteringsavtal” mellan Conscriptor och Barn- och Ungdomsmottagningen i Skene, dels en informations-skrift rubricerad ”informationssäkerhet VID DATORN PÅ JOBBET”.

2.2 Yttrande från Styrelsen för Angereds Närsjukhus i Västra Götalandsregionen

I sitt yttrande anförde Styrelsen för Angereds Närsjukhus (ANS) bl.a. följande (omnämnda bilagor har utelämnats):

Överväganden inför köp av tjänst

ANS har skyldighet att säkra att patientdokumentationen är uppdaterad enligt Hälso- och sjukvårdslagen. För att leva upp till de lagstadgade kraven kring patientdokumentationen har verksamheten på ANS varit tvungen att periodvis förstärka bemanningen inom detta område. Det har skett genom köp av tjänst från externt företag.

Överenskommelse hantering av personuppgifter

ANS har tillsammans med Conscriptor upprättat underlag till överenskommelse för hur journaler ska hanteras, (bilaga 2).

Enligt överenskommelsen agerar Conscriptor som personuppgiftsbiträde och ska behandla personuppgifter enligt personuppgiftslagen och har ansvar för att vidta de säkerhetsåtgärder som avses i personuppgiftslagen, 31 §, samt att personuppgifterna behandlas i enlighet med Västra Götalandsregionens informationssäkerhetspolicy.

Conscriptor anger att tjänsten utförs med diktering som överförs krypterad till säker server. Vid journalskrivning på distans sparas ingen känslig information på den lokala datorn, utan bara på den säkra servern/serverklustret. All information hanteras lokalt på den av Västra Götalandsregionen tillhandahållna servermiljön. Conscriptor ska enligt överenskommelsen logga all aktivitet. För ytterligare information om den tekniska lösningen hänvisas till beskrivningen som primärvården lämnat i sitt yttrande, som överensstämmer med teknisk lösning för ANS.

Slutsats

Det finns inte något skäl att tro att gällande sekretessregler enligt överenskommelsen inte har efterlevts.

Till yttrandet hade fogats en handling rubricerad ”Utdrag ur överenskommelse ANS–Conscriptor”.

2.3 Yttrande från Styrelsen för Stockholms läns sjukvårdsområde (SLSO) i Stockholms läns landsting

I sitt yttrande anförde Styrelsen för SLSO bl.a. följande:

Avtal tecknades med Conscriptor AB den 1 december 2009 efter en förenklad upphandling där ifrågasvarande leverantör lämnade det bästa anbudet på efterfrågade tjänster.

I avtalet med leverantören regleras skyldigheten att upprätthålla sekretess och säkerhet kring patienten på följande sätt:

”Avroparen är personuppgiftsansvarig. Leverantören agerar personuppgiftsbiträde och behandlar personuppgifter utifrån innehållet i detta ramavtal och dess bilagor. Leverantören tillser att behandling av personuppgifter sker enligt personuppgiftslagen (SFS 1998:204). Leverantören ansvarar för i sitt arbete som personuppgiftsbiträde att vidta de säkerhetsåtgärder som avses i Personuppgiftslagen, 31 § första stycket”.

För att säkerhetsställa att denna paragraf följs har leverantören upprättat följande rutiner:

Samtliga anställda genomgår en internutbildning där de bland annat går igenom hantering av login, sekretess och rutiner för PUL uppgifter.

Leverantören har tydliga anställningsbevis som muntligen går igenom med var och en innan ny personal skriver under dessa. Detta görs för att säkerställa att personen förstår innebörden av det ingångna avtalet. I avtalet regleras sekretess samt rutiner för hantering av de uppgifter man får tillgång till i sin anställning. Samtliga anställda har ett anställningsbevis där bland annat sekretessen regleras. Sekretessen gäller även när personalen undantagsvis arbetar från sitt hemmakontor/distansarbetsplats. Avtalet som tecknas med den anställde ser något olika ut beroende på befattning men under stycke ”Sekretess” är alla avtal exakt likalydande:

Sekretessbestämmelse i anställningsbevis:

”Medarbetaren är informerad om att Bolaget i sin verksamhet agerar personuppgiftsbiträde för sina uppdragsgivare. Såsom varandes personuppgiftsbiträde har Bolaget åtagit sig dels för Bolagets räkning, dels för sin personals räkning att efterleva lagar kring hantering av personuppgifter inom hälso- och sjukvårdsområdet.

Medarbetaren är införstådd av vikten av dessa åtagande och åtar sig att följa desamma. Vidare kommer Medarbetaren löpande delges Bolagets samt Bolagets uppdragsgivares informationssäkerhetspolicies och det åligger Medarbetaren att agera i enlighet med dessa och meddela Bolaget vid misstanke av bristande uppfyllelse avseende dessa.

Medarbetaren är medveten om att tjänsten innebär tillgång och hantering av personuppgifter som skyddas av bland annat, men inte uteslutande av, Offentlighets- och sekretesslagens (2009:400), Patientdatalagen (2008:355) och Personuppgiftslagen (1998:204). Tystnadsplikt gäller således avseende all information och uppgifter som Medarbetaren har fått tillgång till genom anställningen på Bolaget.

Vid varje överträdelse av denna sekretessbestämmelse skall Medarbetaren till Bolaget utge ett skadestånd motsvarande den skada företaget kan dokumentera att det lidit på grund av överträdelsen. Det åligger företaget att påvisa skadans omfattning”.

Conscriptor ansluter direkt mot SLSOs datalager dvs. ingen data flyttas över till leverantören, utan alla journaler, ljudfiler etc. hanteras uteslutande lokalt hos SLSO med landstingets krav på autentisering. Leverantören använder sig av virtuella datorer på en plattform som heter VirCon 5.5. Miljön driftas i ett datacenter med mycket hög säkerhet och har en sådan karaktär att det är säkerhetsklassat dvs. det ingår som ett objekt som har intresse för rikets säkerhet. Ingen lokal data sparas, dvs. det finns inga överlappande lager mellan den lokala klienten och den virtuella maskinen. Leverantören använder vidare sk. ”full end point” kryptering, dvs. det finns en krypterad förbindelse mellan lokal maskin och den virtuella miljön. Ingen lokal anslutning tillåts (går) att ansluta till VirCon 5.5. Därmed går det inte att ansluta en extern skrivare till miljön för lokala utskrifter. Man kan inte heller öppna en webbläsare eller använda ”print Screen” funktioner.

Leverantörens hantering av sekretess för personal enligt beskrivning ovan, i kombination med den säkra datamiljön gör att sekretess kring patienten kan anses vara tillfyllest.

2.4 Yttrande från Socialstyrelsen

Därefter remitterade JO ärendet till Socialstyrelsen och begärde att styrelsen skulle yttra sig. Yttrandet skulle avse frågan om det hade funnits rättsliga förutsättningar för regionen/landstinget att överföra uppgifter om patienter till Conscriptor.

I sitt remissvar anförde Socialstyrelsen bl.a. följande:

Yttrande

De rättsliga förutsättningarna för vårdgivaren att överföra uppgifter om patienter till Conscriptor AB (Härefter Conscriptor) följer av personuppgiftslagen (1998:204). Enligt personuppgiftslagen så finns det en möjlighet för den personuppgiftsansvarige, i detta fall vårdgivaren, att anlita ett personuppgiftsbiträde, Conscriptor, som behandlar personuppgifter för den personuppgiftsansvariges räkning. Även om en personuppgiftsansvarig anlitar ett personuppgiftsbiträde är det alltid den personuppgiftsansvarige som har ansvaret gentemot de registrerade. Personuppgiftsansvaret kan inte överlåtas. Det ligger därigenom ett långtgående ansvar på de vårdgivare som anlitar Conscriptor för att säkerställa och följa upp att sekretessen beaktas och att nödvändiga säkerhetsåtgärder vidtas hos Conscriptor.

Bakgrund

Aktiebolaget Conscriptor har som affärsidé att tillhandahålla läkarsekreterarkompetens på distans som hjälper till med administrationen av patientjournaler när ordinarie personal hos en vårdgivare inte hinner med detta arbete. Conscriptor utför uppdrag åt både sjukhus och vårdcentraler i hela Sverige, bl.a. Karolinska Universitetssjukhuset, Huddinge.

Tillämpliga regler m.m.

Hälso- och sjukvårdslagen och patientsäkerhetslagen.

Vårdgivaren ska enligt 3 kap. 1 § patientsäkerhetslagen (2010:659) planera, leda och kontrollera verksamheten på ett sätt som leder till att kraven på god vård i hälso- och sjukvårdslagen (1982:763) och tandvårdslagen (1985:125) upprätthålls. Det innebär bland annat att vårdgivaren ansvarar för att det finns den personal, de lokaler och den utrustning som behövs för att god vård ska kunna ges. Det är alltså vårdgivaren som ska se till att det finns de resurser som behövs för att journalföringen utförs i enlighet med gällande rätt.

Patientdatalagen

I patientdatalagen (2008:355) regleras vårdgivarens ansvar för behandling av personuppgifter inom hälso- och sjukvården.

Enligt [1 kap.] 4 § patientdatalagen gäller personuppgiftslagen vid sådan behandling av personuppgifter inom hälso- och sjukvården som är helt eller delvis automatiserad eller där uppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier, om inte annat följer av patientdatalagen eller föreskrifter som meddelats med stöd av patientdatalagen. Personuppgiftslagen är således subsidiär till patientdatalagen.

Vårdgivaren ansvarar för att informationshanteringen är organiserad så att den tillgodoser patientsäkerhet och god kvalitet samt främjar kostnadseffektivitet. Personuppgifterna ska utformas och i övrigt behandlas så att patienters och övriga registrerades integritet respekteras. Dokumenterade personuppgifter ska hanteras och förvaras så att obehöriga inte kan ta del av dem (1 kap. 2 §).

Vårdgivaren har följaktligen det yttersta ansvaret för journalföringen och för att personuppgifterna hanteras på ett säkert sätt. Vårdgivaren utövar sitt ansvar genom

att ge direktiv till den egendrivna verksamheten eller genom att anlita uppdragstagare.

Vid vård av patienter ska vårdgivaren enligt 3 kap. 1 § patientdatalagen upprätta en journal för varje patient. Uppgifter som antecknas i en patientjournal ska enligt 3 kap. 9 § patientdatalagen föras in i journalen så snart som möjligt. Vårdgivarens informationssäkerhetspolicy ska också säkerställa att patientuppgifterna är åtkomliga och användbara för den som är behörig, vilket anges i 2 kap. 2 § Socialstyrelsens föreskrifter (SOSFS 2008:14) om informationshantering och journalföring i hälso- och sjukvården.

Det är lämpligt att vårdgivaren anpassar sina rutiner för hur snabbt en journal-anteckning ska föras in i patientjournalen efter behoven i sin verksamhet och de krav på säkerhet som ställs. Vårdgivaren ansvarar för att organisera sin verksamhet så att skyndsamhetskravet kan uppfyllas. Det kan antingen göras genom att se till att det finns tillräckliga resurser och goda rutiner inom verksamheten eller genom att anlita personuppgiftsbiträden.

Personuppgiftslagen

Personuppgiftsansvarig är normalt den juridiska person (till exempel aktiebolag, stiftelse eller förening) eller den myndighet som behandlar personuppgifter i sin verksamhet och som bestämmer vilka uppgifter som ska behandlas och vad uppgifterna ska användas till. Enligt 2 kap. 6 § patientdatalagen är vårdgivaren personuppgiftsansvarig för den behandling av personuppgifter som vårdgivaren utför.

Den personuppgiftsansvarige ska se till att behandlingen av personuppgifter är laglig enligt personuppgiftslagen och patientdatalagen och har till exempel ansvaret för informationssäkerheten och att de registrerade får den information de har rätt till. Personuppgiftsansvaret är straff- och skadeståndssanktionerat.

Personuppgiftsbiträde är enligt 30 § personuppgiftslagen den som behandlar personuppgifter för den personuppgiftsansvariges räkning. Ett personuppgiftsbiträde finns alltid utanför den personuppgiftsansvariges organisation. Ett biträde kan vara en servicebyrå som behandlar personuppgifter på uppdrag av ett aktiebolag eller en myndighet.

Det följer av 30 § personuppgiftslagen att personuppgiftsbiträdet endast får behandla personuppgifterna enligt givna instruktioner från den personuppgiftsansvarige.

Även om en personuppgiftsansvarig anlitar ett personuppgiftsbiträde är det alltid den personuppgiftsansvarige som har ansvaret gentemot de registrerade. Personuppgiftsansvaret kan inte överlåtas. De personer vars uppgifter behandlas har alltid rätt att vända sig till den personuppgiftsansvarige och framställa eventuella krav eller klagomål på felaktig behandling av personuppgifter.

Det ska enligt 30 § finnas ett skriftligt avtal om personuppgiftsbitrådets behandling av personuppgifter för personuppgiftsansvariges räkning. I avtalet ska det särskilt föreskrivas att personuppgiftsbiträdet bara får behandla personuppgifterna i enlighet med instruktioner från den personuppgiftsansvarige och att biträdet måste vidta lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifterna. I 31 § andra stycket ställs krav på att den personuppgiftsansvarige skall förvissa sig om att personuppgiftsbiträdet kan genomföra de säkerhetsåtgärder som måste vidtas och se till att personuppgiftsbiträdet verkligen vidtar åtgärderna. Det är den personuppgiftsansvarige som har ansvaret i förhållande till de registrerade även när ett personuppgiftsbiträde anlitas.

Socialstyrelsens föreskrifter (2008:14) om informationshantering och journalföring i hälso- och sjukvården.

De rubricerade föreskrifterna är tillämpliga vid vårdgivares behandling av personuppgifter i verksamhet som omfattas av hälso- och sjukvårdslagen (1982:763) m.fl. I föreskrifterna finns regler om vårdgivarens ansvar för hanteringen av

patientuppgifter. Vårdgivaren ska enligt 2 kap. 2 § i föreskrifterna ha en dokumenterad informationssäkerhetspolicy och om vårdgivaren använder öppna nät för överföring av patientuppgifter ska denne enligt 2 kap. 5 § i samma föreskrifter ansvara för att överföringen görs så att ingen obehörig kan ta del av uppgifterna och att åtkomst till uppgifterna föregås av stark autentisering.

Vårdgivaren ska i sitt avtal med ett personuppgiftsbiträde se till att lämpliga tekniska och organisatoriska åtgärder vidtas för att skydda de patientuppgifter som behandlas.

Tystnadsplikt

Offentlighets- och sekretesslagen (2009:400) gäller som regel inte den som är anställd i ett privaträttsligt objekt. Det är i stället lämpligt att det enskilda företaget sluter avtal med sina anställda om tystnadsplikt eller att en myndighet ställer upp förbehåll om att uppgifter som arbetstagare som inte är offentliga funktionärer får kännedom om i sin verksamhet inte får röjas för utomstående.

Socialstyrelsens bedömning

Av patientdatalagen framgår att vårdgivaren är personuppgiftsansvarig för den behandling av personuppgifter som vårdgivaren utför. Enligt personuppgiftslagen så finns det en möjlighet för den personuppgiftsansvarige, i detta fall vårdgivaren, att anlita ett personuppgiftsbiträde som behandlar personuppgifter för den personuppgiftsansvariges räkning.

I det aktuella fallet har de berörda vårdgivarna anlitat företaget Conscriptor som personuppgiftsbiträde. Vårdgivarna har alltså inte lämnat ut personuppgifter utan anlitat Conscriptor att utföra behandling av personuppgifter åt dem. Vårdgivarna kan inte överlåta sitt personuppgiftsansvar till personuppgiftsbiträde utan har fortsatt ansvar för de uppgifter som personuppgiftsbiträdet hanterar på deras uppdrag.

Av personuppgiftslagen följer att vårdgivarna ska föreskriva i avtal med personuppgiftsbiträdet att biträdet är skyldigt att vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Det ska till exempel säkerställas att inga obehöriga kan ta del av patientuppgifter när personuppgiftsbiträdets personal arbetar med patientuppgifterna eller lämnar datorn. Det är vårdgivarens ansvar att förvissa sig om att personuppgiftsbiträdets behandling av patientuppgifter är laglig och sker på ett korrekt sätt.

Sekretess är grundläggande inom hälso- och sjukvården för att patienter ska kunna känna förtroende för hälso- och sjukvårdspersonal så att han eller hon vågar lämna alla relevanta uppgifter om sitt hälsotillstånd utan risk för att uppgifterna kan bli åtkomliga för obehöriga. Om detta förtroende sviktar kan risker för patientsäkerheten uppstå.

De vårdgivare som anlitar Conscriptor för att säkerställa och följa upp att sekretessen beaktas och att nödvändiga säkerhetsåtgärder vidtas hos Conscriptor har därför ett långtgående ansvar. Vårdgivaren ska även säkerställa att den personal som personuppgiftsbiträdet anlitar inte röjer för utomstående vad de får kännedom vid behandlingen av patientuppgifterna.

Detta ansvar ska vårdgivaren fullgöra dels genom en avtalsskrivning där kraven framgår tydligt, dels genom uppföljning av hur företaget hanterar uppgifterna i praktiken.

2.5 Yttrande från Datainspektionen

JO begärde även att Datainspektionen skulle yttra sig i frågan om regionens/landstingets överförande av uppgifter om patienter till Conscriptor hade varit förenligt med bestämmelserna om hantering av personuppgifter.

I sitt yttrande anförde Datainspektionen bl.a. följande:

Hänvisningar nedan avser personuppgiftslagen, om inte annat anges.

Inledning

Enligt 2 § personuppgiftsförordningen (1998:1191) är Datainspektionen tillsynsmyndighet enligt personuppgiftslagen. Primärt ingår det inte i vårt myndighetsuppdrag att ta ställning till om de aktuella vårdgivarna på ett korrekt sätt har tillämpat offentlighets- och sekretesslagen (2009:400) eller andra bestämmelser om sekretess eller tystnadsplikt, när de har överfört patientuppgifter till det aktuella företaget.

Att vårdgivarna har tillämpat sådana bestämmelser är dock av avgörande betydelse eftersom en personuppgiftsansvarig alltid ska se till att personuppgifter behandlas bara om det är lagligt, 9 § första stycket a). En behandling av personuppgifter i form av en överföring får därför inte utföras om överföringen är i strid med andra bestämmelser som den personuppgiftsansvarige ska tillämpa inom sitt verksamhetsområde och som denne får förutsättas ha kunskap om. Sekretess- och tystnadspliktsbestämmelser är ett exempel på andra bestämmelser som den personuppgiftsansvarige behöver beakta som ett led i frågan om laglighet.

Vår översiktliga bedömning är att 10 kap. 2 § offentlighets- och sekretesslagen eventuellt kan utgöra en sekretessbrytande bestämmelse som är tillämplig i det här fallet, men det ställningstagandet torde närmast vara en fråga för JO. I ett bredare integritetsperspektiv tror vi att det är värdefullt för vårdgivare och patienter att JO belyser frågan.

Några relevanta exempel på dataskyddsbestämmelser

Av JO bifogade yttranden är förknippade med möjligheten att anlita ett personuppgiftsbiträde. Vi vill därför framhålla följande.

Gällande dataskyddet utgår personuppgiftslagen från att en personuppgiftsansvarig med beaktande av vissa krav kan anlita ett personuppgiftsbiträde för att behandla personuppgifter för den personuppgiftsansvariges räkning.

Enligt 30 § första stycket får den eller de personer som arbetar under personuppgiftsbiträdets eller den personuppgiftsansvariges ledning behandla personuppgifter bara i enlighet med instruktioner från den personuppgiftsansvarige. Enligt 30 § andra stycket personuppgiftslagen ska det finnas ett skriftligt avtal där det ska föreskrivas att personuppgiftsbiträdet får behandla personuppgifter bara i enlighet med instruktioner från den personuppgiftsansvarige och att personuppgiftsbiträdet är skyldigt att vidta de åtgärder som avses i 31 § första stycket personuppgiftslagen.

Av sist nämnda bestämmelse framgår följande. En personuppgiftsansvarig ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Dessa åtgärder ska åstadkomma en säkerhetsnivå som är lämplig med beaktande av de tekniska möjligheter som finns, vad det skulle kosta att genomföra åtgärderna, de särskilda risker som finns med behandlingen av personuppgifterna och hur pass känsliga de behandlade personuppgifterna är.

En vårdgivare måste också förvissa sig om att personuppgiftsbiträdet kan genomföra de säkerhetsåtgärder som måste vidtas och se till att personuppgiftsbiträdet verkligen vidtar säkerhetsåtgärderna. Det framgår av 31 § andra stycket.

När det gäller patientdatalagen (2008:355) och patientuppgifter är det viktigt att notera att det finns *uttryckliga krav* på säkerhetsåtgärder som en vårdgivare ska vidta. Någon bedömning enligt 31 § första stycket personuppgiftslagen om *lämpliga* säkerhetsåtgärder behövs således inte i just de fall det finns uttryckliga krav på att vidta säkerhetsåtgärder, jämför med 1 kap. 4 § patientdatalagen.

De *uttryckliga kraven* på säkerhetsåtgärder som typiskt sett blir aktuella för en vårdgivare som överför patientuppgifter till ett personuppgiftsbiträde är

- behörighetstilldelning/-styrning, 4 kap. 2 § patientdatalagen och 2 kap. 6 § Socialstyrelsens föreskrifter Informationshantering och journalföring i hälso- och sjukvården SOSFS 2008:14
- åtkomstkontroll, inklusive logguppföljning, 4 kap. 3 § patientdatalagen och 2 kap. 11 § SOSFS 2008:14, samt
- stark autentisering och kryptering när patientuppgifter överförs i öppet nät, 2 kap. 5 § första stycket SOSFS 2008:14, ändrad SOSFS 2011:8.

I det sammanhang som omfattas av SOSFS 2008:14 avses med patientuppgifter behandling av patienters personuppgifter, 1 kap. 2 § första stycket SOSFS 2008:14. Med stark autentisering avses autentisering som innebär att identiteten kontrolleras på två olika sätt, 1 kap. 3 § SOSFS 2008:14.

Datainspektionen anser att det är särskilt viktigt att en vårdgivare ger sitt personuppgiftsbiträde tydliga instruktioner enligt 30 § andra stycket om de *uttryckliga* säkerhetsåtgärder som biträdet måste vidta och som är förknippade med just det uppdrag som vårdgivaren ger till sitt personuppgiftsbiträde gällande personuppgiftsbehandling. Tillkommer gör självklart också de säkerhetsåtgärder som bygger på en bedömning enligt 31 § personuppgiftslagen, som beskrivits ovan.

På det underlag vi har fått från JO kan vi inte dra några säkra slutsatser om vårdgivarna har levt upp till bestämmelserna i patientdatalagen och personuppgiftslagen. Våra exempel ovan är inte heller uttömmande.

Som en del i vårt yttrande bifogar vi en skrivelse och ett beslut i ett tillsynsärende där vi tillsynsvis kontrollerat en vårdgivare som låter egna medicinska sekreterare utföra arbete inom hälso- och sjukvården från hemmet (Datainspektionens ärende 949-2012). Det är inte fråga om anlitande av ett personuppgiftsbiträde. Ett fokus i tillsynen är 2 kap. 5 § första stycket SOSFS 2008:14.

De berörda nämnderna fick tillfälle att kommentera remissvaren från Socialstyrelsen och Datainspektionen.

AA kommenterade remissvaren. Han bifogade en tidningsartikel.

3 Bedömning

3.1 Inledning

När uppgifter om patienter inom hälso- och sjukvården journalförs behandlas information om patienterna (personuppgifter) som är mycket känslig ur integritets-synpunkt. Inom hälso- och sjukvården skyddas sådana uppgifter genom dels bestämmelser om sekretess/tystnadsplikt, dels bestämmelser om hur personuppgifter får behandlas.

Bestämmelser om sekretess finns främst i offentlighets- och sekretesslagen (2009:400), OSL. I den lagen regleras bl.a. när en uppgift omfattas av sekretess och när en sådan uppgift kan lämnas ut till en annan myndighet eller till enskilda, t.ex. ett företag. I OSL regleras också frågan om tystnadsplikt för personal inom den allmänna hälso- och sjukvården.

Regler om behandling av personuppgifter (bl.a. journalföring) inom hälso- och sjukvården finns framför allt i patientdatalagen (2008:355) och personuppgiftslagen (1998:204), PuL. Patientdatalagen innehåller särskilda regler om behandling av personuppgifter inom hälso- och sjukvården, medan det i PuL finns allmänna regler om behandling av personuppgifter. Regleringen innebär att PuL ska

tillämpas i sådana fall där frågan inte är reglerad i patientdatalagen, eller i en annan lag eller i en förordning (se 2 § PuL och 1 kap. 4 § patientdatalagen). Vårdgivare måste även beakta bl.a. Socialstyrelsens föreskrifter (SOSFS 2008:14) om informationshantering och journalföring i hälso- och sjukvården.

En behandling av personuppgifter är tillåten bara om den är förenlig med reglerna i OSL (jfr 9 § första stycket a PuL, som berörs i Datainspektionens yttrande). En grundläggande förutsättning för en överföring av patientuppgifter för journalföring är således att regelverket om sekretess har beaktats.

Inom den allmänna hälso- och sjukvården är det vårdgivaren (inom ett landsting/en region, ofta en nämnd) som ansvarar för att den sekretess som gäller för uppgifter om enskilda patienter upprätthålls. Vårdgivaren är också personuppgiftsansvarig för den behandling av personuppgifter som vårdgivaren utför (2 kap. 6 § patientdatalagen).

I det här ärendet aktualiseras frågan om en vårdgivare uppfyller detta ansvar när vårdgivaren anlitar ett företag för hjälp med journalföring av patientuppgifter. Under utredningen har JO begärt in yttranden från tre vårdgivare som har anlitat samma företag. Utgångspunkten för de avtal som har ingåtts mellan de berörda nämnderna (styrelserna är nämnder i kommunallagens [1991:900] mening) och företaget är att företaget i förhållande till vårdgivaren agerar i egenskap av personuppgiftsbiträde. Ett sådant biträde behandlar personuppgifter för den personuppgiftsansvariges (dvs. vårdgivarens) räkning (3 § PuL).

Avtalen innebär kortfattat följande. Vårdgivaren anlitar företaget för hjälp med journalföring. Företagets personal (läkarsekreterare) utför den faktiska behandlingen av personuppgifter som innefattar journalföringen. Vårdgivaren ger läkarsekreterarna behörighet att logga in i vårdgivarens elektroniska journalsystem. Inlästa uppgifter (diktat) om patienterna blir därmed tillgängliga för läkarsekreterarna som lyssnar av diktaten och skriver in uppgifterna i patientens journal. Läkarsekreterarna utför sitt arbete utanför vårdgivarens lokaler, i vissa fall från sitt hem. Såvitt framkommit har vårdgivarna inte någon direkt relation till läkarsekreterarna och vet inte heller vem hos företaget som kommer att journalföra en viss uppgift. Som jag uppfattat saken innebär den tekniska lösningen att uppgifterna behandlas enbart elektroniskt och att de inte vid något tillfälle lagras utanför landstingets/regionens it-system.

Min granskning är i första hand inriktad på frågan om det är förenligt med sekretesslagstiftningen att landstinget/regionen på detta sätt lämnar ut/överför patientuppgifter till den personal (läkarsekreterare) som är anställd hos personuppgiftsbiträdet och som utför journalföringen. Jag berör dock även vissa aspekter av regelverket om behandling av personuppgifter som har betydelse i sammanhanget.

Att regelverket om behandling av personuppgifter, utöver det som framgår i det följande, ställer långtgående krav på framför allt den personuppgiftsansvarige

framgår av yttrandena från Socialstyrelsen och Datainspektionen. En vårdgivare som anlitar ett personuppgiftsbiträde för journalföring måste beakta en rad frågor som gäller såväl tekniska som organisatoriska aspekter. I Socialstyrelsens yttrande finns även en redovisning av kraven på vårdgivarens journalföring i sig.

3.2 Regler om sekretess och tystnadsplikt m.m.

3.2.1 Sekretess inom den allmänna hälso- och sjukvården m.m.

Inom den allmänna 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 denne lider men (25 kap. 1 § OSL). Sekretessen gäller både mot enskilda och mot andra myndigheter (8 kap. 1 § OSL).

Det s.k. omvända skaderekvisitet som finns i 25 kap. 1 § OSL innebär att uppgifter om en enskilds personliga förhållanden i en patientjournal i princip enbart kan lämnas ut med den enskildes samtycke (10 kap. 1 § OSL) eller med stöd i OSL eller en lag eller förordning som OSL hänvisar till (8 kap. 1 § OSL).

När sekretessbelagda uppgifter behandlas inom den allmänna hälso- och sjukvården gäller vidare följande.

Av 2 kap. 1 § OSL följer att det är förbjudet för såväl myndigheter som vissa personer (som har tystnadsplikt) att röja uppgifter som är sekretessbelagda enligt OSL. Ett röjande kan ske muntligen, genom ett utlämnande av en allmän handling eller på något annat sätt (3 kap. 1 § OSL).

Av den följande redovisningen kommer det att framgå att vårdgivarens egen personal har tystnadsplikt enligt OSL som omfattar de (sekretessbelagda) uppgifter om en patient som personalen får reda på (t.ex. i samband med journalföring). En fråga i detta ärende är om personuppgiftsbiträdets personal (läkarsekreterarna) har tystnadsplikt enligt OSL när de utför journalföring enligt avtalen. I så fall skulle – något förenklat – journalföring enligt avtalen inte innebära att sekretessbelagda uppgifter röjs. Jag uppehåller mig därför i det följande först vid frågan om personalen hos biträdet omfattas av tystnadsplikt enligt OSL och vid vissa närliggande frågor som rör andra former av tystnadsplikt än den som följer av OSL. Därefter redovisar jag vissa sekretessbrytande bestämmelser som innebär att ett utlämnande av en uppgift i vissa fall är möjligt även om uppgiften är sekretessbelagd, och går in på frågan om de är tillämpliga i det här sammanhanget.

3.2.2 Bestämmelser om tystnadsplikt för personal inom hälso- och sjukvården m.m.

3.2.2.1 Straffsanktionerad tystnadsplikt

Personal inom såväl den allmänna som den enskilda hälso- och sjukvården omfattas av bestämmelser om tystnadsplikt. Den som omfattas av en sådan tystnadsplikt och som felaktigt röjer en uppgift kan i vissa fall dömas för brott mot tystnadsplikt.

Straffbestämmelsen finns i 20 kap. 3 § brottsbalken. I den föreskrivs att om någon röjer en uppgift, som han är skyldig att hemlighålla, eller om han olovligen utnyttjar en sådan hemlighet, ska han, om inte gärningen är straffbelagd på annat sätt, dömas för *brott mot tystnadsplikt* till böter eller fängelse i högst ett år. Enligt andra stycket ska den som av oaktsamhet begår en gärning som avses i första stycket, dömas till böter. I ringa fall ska dock inte dömas till ansvar.

3.2.2.2 *Tystnadsplikt för personal inom den enskilda hälso- och sjukvården*

När det gäller hälso- och sjukvårdspersonal inom den enskilda hälso- och sjukvården finns bestämmelsen om tystnadsplikt i 6 kap. 12 § patientsäkerhetslagen (2010:659). Enligt denna får den som tillhör eller har tillhört hälso- och sjukvårdspersonalen inom den enskilda hälso- och sjukvården inte obehörigen röja vad han eller hon i sin verksamhet har fått veta om en enskilds hälsotillstånd eller andra personliga förhållanden. Vem som i detta avseende utgör hälso- och sjukvårdspersonal framgår av 1 kap. 4 § patientsäkerhetslagen. Personalen hos det aktuella personuppgiftsbiträdet omfattas inte av denna bestämmelse.

3.2.2.3 *Tystnadsplikt för personal inom den allmänna hälso- och sjukvården*

För personal inom den allmänna hälso- och sjukvården finns tystnadspliktsbestämmelsen i 2 kap. 1 § andra stycket OSL. I denna föreskrivs ett förbud att röja uppgifter enligt OSL. Förbudet gäller för personer som har fått kännedom om uppgiften genom att för det allmännas räkning delta i en myndighets verksamhet

- 1) på grund av anställning eller uppdrag hos myndigheten,
- 2) på grund av tjänsteplikt, eller
- 3) på annan liknande grund.

Bestämmelsen behandlas i förarbetena till den tidigare gällande sekretesslagen (1980:100), prop. 1979/80:2 Del A s. 126 f.

Tystnadsplikten enligt 1) tar, utöver anställda, sikte på personer som utför uppdrag hos en myndighet och som har en sådan anknytning till myndigheten att de kan sägas delta i dennas verksamhet. Det är bara uppdragstagare som är fysiska personer som i sekretesshänseende ska jämföras med arbetstagare hos myndigheten. Exempel på sådana uppdragstagare som är tänkta att omfattas av bestämmelsen är kontaktpersoner inom socialtjänsten och olika slag av konsulter.

Det kan mot denna bakgrund konstateras att personalen hos personuppgiftsbiträdet inte omfattas av tystnadsplikt enligt 1). Bestämmelsen om tystnadsplikt på grund av tjänsteplikt enligt 2) är inte heller tillämplig i det här fallet.

Om deltagande enligt 3) – *på annan liknande grund* – anfördes bl.a. följande i de nämnda förarbetena (a. prop. Del A s. 128; jfr Del B s. 190–191):

Sekretesslagen gäller i princip inte den som är anställd hos privat rättssubjekt. Om myndigheten har träffat avtal t.ex. med ett enskilt företag, kan det emellertid som framhålls i promemorian i undantagsfall te sig naturligt att arbetstagare hos motparten får lyda under bestämmelse i sekretesslagen. Jag syftar här bl.a. på sådana

fall som riksrevisionsverket tar upp i sitt remissyttrande, nämligen då arbetstagaren ställs till myndighetens förfogande och deltar i dess verksamhet på samma sätt som om myndigheten hade ingått uppdragsavtal med vederbörande själv. Med tanke på sådana och liknande fall gäller 7 § [*motsvarar 6 § i lagen; JO:s anm.*] även den som på "annan liknande grund" deltar i myndighets verksamhet.

JO har tidigare behandlat förutsättningarna för en socialnämnd att anlita ett privaträttsligt subjekt som utredare inom socialtjänsten (JO 2001/02 s. 250, dnr 2598-2000 och 2617-2000). I beslutet anfördes i fråga om sekretess bl.a. följande (1 kap. 6 § sekretesslagen, 1980:100, motsvaras i dag av 2 kap. 1 § OSL):

Ett bolag kan inte ges i uppdrag att utföra en utredning för socialnämndens räkning. Däremot kan det finnas utrymme för socialnämnden att träffa ett avtal med ett bolag om att bolaget skall ställa en viss person till nämndens förfogande. En sådan person kan nämligen i vissa situationer omfattas av sekretesslagens regler. Vid tillkomsten av sekretesslagen uttalades härom bl.a. följande (prop. 1979/80:2 del A s. 128; jfr prop. 1981/82:186 s. 41).

– – – [*Här återges det förarbetsuttalande som har redovisats ovan.*]

Att ett bolag åtar sig att ställa en person till socialnämndens förfogande innebär inte att den personen har ett uppdrag hos myndigheten i den mening som begreppet har i 1 kap. 6 § SekrL. Däremot kan en sådan person vid tillämpning av sekretesslagen kunna anses som en offentlig befattningshavare om han på "annan liknande grund" deltar i myndighetens verksamhet. Om så är fallet bör han kunna likställas med s.k. osjälvständiga eller beroende uppdragstagare även i de hänseenden jag har behandlat tidigare. Enligt min mening torde det därför finnas utrymme för en socialnämnd att till sig knyta en "utredare" genom ett avtal med ett bolag om att bolaget ställer personen till nämndens förfogande. En förutsättning härför är att utredaren, om uppdragsavtal hade träffats med honom själv, varit att betrakta som en befattningshavare vid nämndens förvaltning.

I konsekvens med vad som har anförts får ett avtal, enligt vilket ett bolag åtar sig att ställa en "utredare" till nämndens förfogande, inte utformas så att det ger bolaget rätt att avgöra vem som skall utföra utredningen utan det måste bestämmas genom avtalet. Om den som skall utföra utredningen inte har deltagit vid avtalets tillkomst måste socialnämnden dessutom träffa en särskild överenskommelse med denne rörande utredningens utförande. I annat fall kan inte nämnden vara förvissad om att utredaren är införstådd med under vilka förhållanden som han bedriver sitt arbete. Enligt min mening är det en lämplig ordning att den som skall utföra en utredning på uppdrag av socialnämnden alltid erhåller någon form av förordnande av socialnämnden.

När det gäller frågan om huruvida vårdgivarnas avtal med personuppgiftsbiträdet innebär att bitrådets personal kan omfattas av tystnadsplikt på *annan liknande grund* vill jag anföra följande.

Eftersom den personal som utför journalföringen är anställd i ett företag (dvs. ett privat rättssubjekt) är utgångspunkten att de inte omfattas av tystnadsplikt enligt OSL. De aktuella avtalen innebär att vårdgivaren köper en tjänst – journalföring – av företaget. Enligt avtalen är vårdgivaren personuppgiftsansvarig medan företaget agerar som ett personuppgiftsbiträde. Ett personuppgiftsbiträde finns alltid utanför den personuppgiftsansvariges egen organisation. En anställd eller någon annan som behandlar personuppgifter under den personuppgiftsansvariges direkta ansvar är inte ett personuppgiftsbiträde (jfr Personuppgiftslagen – En kommentar, Zeteo, 25 september 2013, kommentaren till 3 § PuL).

Avtalsparternas avsikt har av allt att döma inte varit att biträdet ska ställa personal till de berörda nämndernas förfogande på ett sätt som innebär att personalen skulle omfattas av tystnadsplikt enligt OSL. Såvitt framgår av remissvaren har nämnderna inte heller utgått från att bitrådets personal skulle ha tystnadsplikt enligt OSL. Att vårdgivaren ensam bestämmer över ändamålen i sig med den aktuella personuppgiftsbehandlingen och i vissa avseenden ska ställa organisatoriska och tekniska krav på biträdet (jfr 30–31 §§ PuL) förändrar inte den bild som avtalen ger av vilken relation mellan bitrådets personal och vårdgivaren som har varit avsedd.

Det verkar inte heller som om enskilda läkarsekreterare hos företaget ställs till vårdgivarens förfogande i praktiken. Såvitt framkommit bestämmer inte vårdgivaren vem hos biträdet som ska utföra journalföringen, vet inte på förhand vem som kommer att behandla en viss uppgift och har inte heller i övrigt något direkt inflytande över det arbete som sekreteraren utför. Det finns inte någon form av överenskommelse eller avtal mellan vårdgivaren och den enskilde läkarsekreteraren.

I dokumentet ”Utdrag ur överenskommelse ANS–Conscriptor”, som styrelsen för ANS har gett in tillsammans med sitt remissvar, anges att ”Conscriptor garanterar att bara namngivna och av Kunden godkända läkarsekreterare hos Conscriptor får tillgång till Kundens data [...]”.

Även om vårdgivaren får denna information från företaget skiljer sig omständigheterna i det här fallet på avgörande punkter från den situation som behandlades i JO 2001/02 s. 250. Detta inte minst eftersom de aktuella avtalen innebär att den personal som behandlar uppgifterna utför sitt arbete i anledning av sin arbetsgivares ställning som personuppgiftsbiträde. Vad som har kommit fram innebär inte att företagets personal kan anses ha en sådan relation till vårdgivarens verksamhet att de omfattas av tystnadsplikt på *annan liknande grund* (jfr i denna fråga JO 1982/83 s. 238, dnr 149-1980, som jag återkommer till nedan).

Sammanfattningsvis gör jag alltså bedömningen att personalen hos personuppgiftsbiträdet inte omfattas av någon sådan straffsanktionerad tystnadsplikt som följer av 2 kap. 1 § andra stycket OSL.

3.2.3 *Gäller någon form av tystnadsplikt för personalen (läkarsekreterare) som utför journalföringen hos personuppgiftsbiträdet?*

Den personal hos ett personuppgiftsbiträde som behandlar uppgifter åt en vårdgivare kan omfattas av andra former av tystnadsplikt än sådan som följer av OSL eller patientsäkerhetslagen. Avtalen mellan företaget och läkarsekreterarna innehåller en klausul om tystnadsplikt. Dessutom följer en sorts tystnadsplikt av reglerna om behandling av personuppgifter inom hälso- och sjukvården. Dessa former av tystnadsplikt är inte straffsanktionerade enligt 20 kap. 3 § brottsbalken, men är ändå av intresse i det här sammanhanget eftersom de kan beaktas vid prövningen av om ett utlämnande av en uppgift innebär men för den som skyddas av sekretessen. Jag återkommer nedan, under rubriken Sammanfattande

synpunkter, till min syn i denna fråga. Jag vill dock här kort beskriva dessa ”alternativa” tystnadsplikter.

3.2.3.1 *Avtalsreglerad tystnadsplikt*

I förarbetena till den tidigare gällande sekretesslagen, 1980:100 (prop. 1981/82:186 s. 41–42) anfördes bl.a. följande (den bestämmelse som nämns motsvaras i dag av 10 kap. 14 § OSL, som jag berör längre fram i beslutet):

Mot bakgrund av det anförda kan konstateras att t.ex. personal från en kontoristförening eller ett bevakningsföretag som regel inte torde vara bundna av sekretesslagen. Jag vill emellertid erinra om att det oftast är möjligt att undvika olägenheter som kan uppkomma till följd härav antingen genom att det enskilda företaget sluter avtal med sina anställda om tystnadsplikt eller genom att en myndighet ställer upp förbehåll om att uppgifter som arbetstagare som inte är offentliga funktionärer får kännedom om i sin verksamhet inte får röjas för utomstående (jfr 14 kap. 9 § SekrL). Detta förfarande kan tillämpas t.ex. när en myndighet anlitar en skrivbyrå för utskrift av handlingar som innehåller sekretessbelagda uppgifter.

Av yttrandet från SLSO framgår hur tystnadsplikten är reglerad i avtalen mellan personuppgiftsbiträdet och den personal hos biträdet som utför journalföringen. Tystnadsplikten omfattar de uppgifter som den personen behandlar i anledning av företagets uppdrag som personuppgiftsbiträde.

Vid en överträdelse av en avtalsreglerad tystnadsplikt är den ”sanktion” mot den personal som brutit mot tystnadsplikten den som kan följa av avtalen. Detta är i första hand en fråga mellan avtalsparterna, dvs. arbetsgivaren och arbetstagaren. Av den aktuella avtalsklausulen framgår att personalen hos biträdet kan bli skyldig att betala skadestånd till företaget, för den eventuella skada som företaget lider på grund av att uppgifter har röjts.

3.2.3.2 *En form av tystnadsplikt följer av reglerna om behandling av personuppgifter*

När en vårdgivare anlitar ett personuppgiftsbiträde för behandling av patientuppgifter är det vårdgivaren som är ansvarig om behandlingen hos biträdet sker i strid med bestämmelserna om hur personuppgifter får behandlas. Ansvariet innebär bl.a. att vårdgivaren som personuppgiftsansvarig ska ersätta den registrerade (t.ex. en patient) för skada och kränkning av den personliga integriteten som en behandling av personuppgifter i strid med patientdatalagen eller PuL har orsakat. Detta framgår av 10 kap. 1 § patientdatalagen och 48 § PuL.

I detta sammanhang är det av intresse att det av 30 § PuL följer en form av tystnadsplikt för t.ex. den som är anställd hos ett personuppgiftsbiträde och som alltså behandlar personuppgifter för den personuppgiftsansvariges räkning. Detta eftersom personuppgifterna bara får behandlas i enlighet med den personuppgiftsansvariges instruktioner. Ett muntligt eller ett skriftligt utlämnande av personuppgifter till tredje man innebär en ”behandling” av uppgiften, jfr 3 § PuL. I förarbetena till PuL anfördes bl.a. följande om detta (prop. 1997/98:44 s. 91):

Skulle någon som arbetar för den personuppgiftsansvarige lämna ut personuppgifter i strid med vad som sålunda gäller, är det den personuppgiftsansvarige som bär det rättsliga ansvaret gentemot den registrerade [...]. I vilken utsträckning den personuppgiftsansvarige i sin tur kan vidta någon åtgärd mot den som lämnade ut uppgiften i strid med givna instruktioner framgår av de bestämmelser som reglerar förhållandet mellan den personuppgiftsansvarige och medhjälparen, t.ex. avtalet med ett personuppgiftsbiträde eller arbetsrättsliga bestämmelser [...]. De allmänt hållna bestämmelserna i den nya lagen innebär inte en sådan plikt att hemlighålla uppgifter som medför att straffstadgandet om brott mot tystnadsplikt i 20 kap. 3 § brottsbalken kan bli tillämpligt.

3.3 Sekretessbrytande bestämmelser i OSL

Om en uppgift är sekretessbelagd får den som huvudregel inte röjas för enskilda eller för andra myndigheter (8 kap. 1 § OSL). I 10 kap. OSL finns dock vissa undantag från huvudregeln – sekretessbrytande bestämmelser – som innebär att uppgiften kan lämnas ut även om den är sekretessbelagd.

3.3.1 *Den sekretessbrytande bestämmelsen om nödvändigt utlämnande i 10 kap. 2 § OSL*

Enligt 10 kap. 2 § OSL hindrar inte sekretess att en uppgift lämnas till en enskild, om det är nödvändigt för att den utlämnande myndigheten ska kunna fullgöra sin verksamhet. Bestämmelsen innebär att det är tillåtet att lämna ut uppgifter även om det innebär skada eller men för den enskilde.

Syftet med bestämmelsen är att förhindra att sekretessregleringen gör det omöjligt för en myndighet och dess personal att sköta de uppgifter som myndigheten har ansvar för. Sekretessen får efterges bara i sådana fall då ett utlämnande av sekretessbelagda uppgifter är en nödvändig förutsättning för att myndigheten ska kunna fullgöra ett visst åtagande (se Offentlighets- och sekretesslagen, Zeteo, 1 juli 2013, kommentaren till 10 kap. 2 § OSL, se även Jesper Ekroths och Therése Fridström Montoyas artikel i FT 2008 s. 153).

Av förarbetena framgår att bestämmelsen ska tillämpas restriktivt. Enbart en bedömning att effektiviteten i myndighetens handlande sätts ner genom en föreskrift om sekretess får inte leda till att sekretessen åsidosätts (jfr prop. 1979/80:2 Del A s. 465 och 494). Som exempel på fall där ett utlämnande med stöd av bestämmelsen kan ske från en myndighet till en enskild nämns ”delgivning med part och annan föreskriven underrättelse till enskild som ett led i behandlingen av ett ärende” (a. prop. s. 122).

I ett äldre beslut, JO 1982/83 s. 238, dnr 149-1980, fann JO att 1 kap. 5 § sekretesslagen, 1980:100 (numera 10 kap. 2 § OSL), möjliggjorde att skattemyndigheter i vissa fall kunde lämna ut sekretessbelagda uppgifter till privata dataföretag för registrering. I det aktuella fallet utnyttjades privata dataföretag för registrering av deklarerationer. Bedömningen i ärendet har ifrågasatts bl.a. i den ovan nämnda artikeln i FT.

Utgångspunkten är alltså att bestämmelsen ska tillämpas restriktivt. I praktiken handlar det om situationer av undantagskaraktär.

En vårdgivare är ansvarig för att det finns de resurser som behövs för att journalföring ska kunna utföras i enlighet med gällande rätt. En vårdgivare måste således anpassa och organisera sin verksamhet i enlighet med detta.

Av remissvaren framgår att vårdgivarnas behov av extern hjälp med journalföring uppkommer när den ordinarie personalen hos vårdgivaren inte hinner med. Det har inte kommit fram något som tyder på att vårdgivarna i och för sig skulle ha varit förhindrade att lösa journalföringen på ett sätt som inte hade riskerat att komma i konflikt med sekretessbestämmelserna. Det hade exempelvis kunnat ske genom en omfördelning av befintlig personal eller genom anställning av ny personal. Att avtalen kan ha inneburit en effektivisering av vårdgivarens journalföring i samband med att arbetsläget har varit ansträngt innebär, som framgår av förarbetsuttalandet ovan, inte i sig att bestämmelsen blir tillämplig. Det kan således enligt min mening inte anses ha varit fråga om ett sådant ”nödvändigt utlämnande” som medför att bestämmelsen i 10 kap. 2 § OSL kan tillämpas.

3.3.2 Den sekretessbrytande bestämmelsen om utlämnande med förbehåll i 10 kap. 14 § OSL

En annan sekretessbrytande bestämmelse finns i 10 kap. 14 § OSL. Genom denna ges myndigheten en möjlighet att lämna ut en uppgift trots att den är sekretessbelagd. En förutsättning är att myndigheten ställer upp ett förbehåll i förhållande till den som tar emot uppgiften. Förbehållet kan avse ett förbud (för mottagaren) att lämna uppgiften vidare eller utnyttja den. Myndigheten måste göra bedömningen att förbehållet undanröjer den risk för men eller skada som utan förbehållet skulle hindra att uppgiften lämnas ut. Den som bryter mot ett förbehåll som har meddelats med stöd av bestämmelsen kan dömas för brott mot tystnadsplikt enligt 20 kap. 3 § brottsbalken.

JO har uttalat sig om förfarandet när ett utlämnande med förbehåll sker, bl.a. i beslutet JO 1992/93 s. 197, dnr 145-1990. I ärendet, som gällde klagomål mot polisen, anförde JO bl.a. följande:

Bedöms en av sekretess omfattad handling kunna lämnas ut med förbehåll måste utlämnandet i varje enskilt fall föregås av ett beslut i saken som skall dokumenteras i polisärendet. Ett sådant beslut skall ange vilken handling det är fråga om, vem handlingen lämnas ut till och som därmed är bunden av förbehållet beträffande just den handlingen och vad förbehållet har för innebörd.

Uttalandet överensstämmer med min syn på vilka krav som en tillämpning av bestämmelsen ställer. Som har framgått finns det inte utrymme för en myndighet att meddela generella förbehåll (jfr även bl.a. JO 1994/95 s. 574, dnr 2079-1993).

4 Sammanfattande synpunkter

4.1 Utgångspunkter

Vid journalföring inom hälso- och sjukvården behandlas uppgifter som många gånger är av mycket känsligt slag. Socialstyrelsen framhåller i sitt yttrande till JO att sekretessen är av grundläggande betydelse för att patienter ska kunna känna förtroende för hälso- och sjukvårdspersonalen. Som Socialstyrelsen har anfört kan det uppstå risker för patientsäkerheten om detta förtroende sviktar.

Enligt OSL råder en stark sekretess för uppgifter om patienter inom den allmänna hälso- och sjukvården. För att sekretessen ska upprätthållas är det av central betydelse att hälso- och sjukvårdspersonalen har en tystnadsplikt som omfattar det som den får reda på i samband med vården av en patient.

Som tidigare har angetts är min granskning inriktad på frågan om de berörda vårdgivarna har uppfyllt sitt ansvar för att upprätthålla sekretessen när man har ingått avtal med det aktuella företaget (ett personuppgiftsbiträde) om journalföring.

Avtalen innebär att företaget ska agera som ett personuppgiftsbiträde åt vårdgivaren. Ett personuppgiftsbiträde och bitrådets personal arbetar nära den personuppgiftsansvarige vårdgivaren; uppgifter får bara behandlas enligt instruktioner från vårdgivaren. Prövningen av om en vårdgivare kan lämna ut sekretessbelagda uppgifter till ett personuppgiftsbiträde eller personal hos bitradet ska emellertid ske på vanligt sätt enligt OSL. Det långtgående tekniska skydd som finns för uppgifterna, förutsatt att regelverket om behandling av personuppgifter har beaktats på ett korrekt sätt, har inte någon direkt betydelse i detta sammanhang. Inte heller det förhållandet att ett utlämnande i PuL:s mening inte sker till en tredje man har någon direkt betydelse.

4.2 Har det funnits rättsliga förutsättningar för vårdgivarna att lämna ut patientuppgifter på det sätt som följer av avtalen?

Jag har redovisat min syn på hur vissa bestämmelser i OSL ska tolkas i det här aktuella sammanhanget. Vad gäller frågan om det har funnits rättsliga förutsättningar för de berörda vårdgivarna att lämna ut uppgifter om patienter på det sätt som följer av avtalen vill jag uppehålla mig vid följande.

Personalen hos personuppgiftsbitradet (läkarsekreterarna) omfattas inte av den tystnadsplikt enligt 2 kap. 1 § andra stycket OSL som skulle ha gällt om vårdgivarens egen personal hade utfört journalföringen. Frågan om huruvida patientuppgifter som finns hos vårdgivaren kan göras tillgängliga för personuppgiftsbitrådets personal är därför i första hand beroende av om ett utlämnande till personalen kan ske utan att det innebär men för den som skyddas av sekretessen. Det är i detta sammanhang som en avtalsreglerad tystnadsplikt och den ”tystnadsplikt” som följer av regelverket om behandling av personuppgifter kan vägas in. Utgångspunkten vid prövningen är emellertid upplevelsen hos den som skyddas av sekretessen (jfr prop. 1979/80:2 Del A s. 80 f.).

I ett ovan redovisat förarbetsuttalande om en liknande situation – en myndighet anlitar en skrivbyrå för utskrift av handlingar som innehåller sekretessbelagda uppgifter – uttalas att problemet med att personalen hos det företag som myndigheten har anlitat inte omfattas av sekretess ”oftast” kan avhjälpas genom att det företag som myndigheten har anlitat har sekretessavtal med sina anställda eller genom att myndigheten lämnar ut uppgifterna med förbehåll enligt (numera) 10 kap. 14 § OSL (prop. 1981/82:186 s. 41–42).

Den personal hos biträdet som utför journalföring åt vårdgivaren har en sådan avtalsreglerad tystnadsplikt som nämns i förarbetsuttalandet. Vid överträdelser av denna kan personalen bli skadeståndsskyldig mot sin arbetsgivare (företaget). Som har framgått följer även av regelverket om behandling av personuppgifter en sorts tystnadsplikt för personalen hos biträdet. Vid överträdelser av denna kan vårdgivaren som personuppgiftsansvarig bli skadeståndsskyldig enligt PuL mot t.ex. en patient.

När uppgifter om patienter lämnas ut till personuppgiftsbiträdes personal för journalföring omfattas de alltså av ett visst skydd. Som har anförts kan tystnadsplikten för den personal som behandlar patientuppgifter antas vara av stor betydelse för bl.a. de berörda patienterna vid deras kontakter med vården. Det blir därför i sammanhanget ofrånkomligt att jämföra med den situationen att uppgifterna behandlas av personal som har en tystnadsplikt enligt 2 kap. 1 § andra stycket OSL.

En principiellt sett mycket viktig skillnad är att personal som har tystnadsplikt enligt OSL (dvs. landstingets/regionens personal) omfattas av ett straffrättsligt ansvar enligt 20 kap. 3 § brottsbalken, medan så inte är fallet när det gäller personalen hos företaget (personuppgiftsbiträdet). Om en tjänsteman hos landstinget/regionen röjer sekretesskyddade patientuppgifter kan alltså hon eller han ställas till ansvar straffrättsligt och dömas för brott mot tystnadsplikt. Det kan inte läkarsekreterarna hos det aktuella företaget i motsvarande situation. Jag bedömer att risken för att patientuppgifter – som ofta är av mycket integritetskänsligt slag – felaktigt lämnas ut är större när den personal som behandlar uppgifterna inte arbetar under en straffsanktionerad tystnadsplikt. Det är därmed enligt min mening tydligt att journalföring enligt avtalen innebär att patientuppgifter har ett svagare skydd än om personal som har tystnadsplikt enligt OSL utför journalföringen.

Mot bakgrund av det nu anförda anser jag att varken den avtalsreglerade tystnadsplikten som gäller för biträdes personal eller den form av tystnadsplikt som följer av regleringen i PuL medför att det kan anses stå klart att patientuppgifter kan lämnas ut till företagets personal för journalföring utan att den enskilde eller någon närstående till denne lider men. Vad som i övrigt har kommit fram, bl.a. att behandlingen enligt avtalen äger rum för vårdgivarens räkning och – som det verkar – under tekniskt säkra förhållanden, ändrar inte den bedömningen.

Min slutsats är således att det inte står klart att ett utlämnande enligt avtalen kan ske utan men för den som skyddas av sekretessen. Sekretessen enligt 25 kap. 1 § OSL hos vårdgivaren gäller alltså i förhållande till personuppgiftsbiträdet och bitrådets personal. Uppgifter om en enskilds personliga förhållanden kan då i princip lämnas ut bara med den enskildes samtycke eller med stöd i OSL eller en lag eller förordning som OSL hänvisar till.

Det har inte påståtts att vårdgivarna hämtat in samtycke till utlämnandet från de personer som skyddas av sekretessen. Som framgått har ett utlämnande av sekretessbelagda uppgifter från vårdgivaren inte kunnat äga rum med stöd av den sekretessbrytande bestämmelsen om nödvändigt utlämnande i 10 kap. 2 § OSL eller haft stöd i en annan lag eller förordning som OSL hänvisar till. I sammanhanget kan tilläggas att den sekretessbrytande bestämmelsen i 10 kap. 14 § OSL inte ger stöd för utlämnande av uppgifter mot generellt uppställda förbehåll.

Sammanfattningsvis gör jag den samlade bedömningen att vårdgivarna inte har haft rättsligt stöd för att på det sätt som skett lämna ut sekretesskyddade uppgifter om patienter för behandling av personuppgiftsbitrådets personal.

4.3 Avslutande synpunkter

Nämndernas remissvar till JO och det som har kommit fram om avtalen ger intryck av att avtalsparterna främst har lagt vikt vid sina respektive roller enligt regelverket om behandling av personuppgifter. Som framgått har emellertid en vårdgivare även ansvar för att hälso- och sjukvårdssekretessen upprätthålls. En behandling av personuppgifter är tillåten bara om den är förenlig med reglerna i OSL. Av nämndernas remissvar framgår inte vilka överväganden som har gjorts i fråga om sekretess. Det är anmärkningsvärt att vårdgivarna inte har ägnat sekretessaspekterna större uppmärksamhet i samband med att de ingått avtalen.

De berörda nämnderna förtjänar allvarlig kritik för att de har ingått avtal som innebär att landstinget och regionen lämnar ut patientuppgifter för journalföring av anställda vid ett företag trots att detta inte är förenligt med regelverket om sekretess. Jag förutsätter att landstinget och regionen beaktar mina uttalanden och vidtar de åtgärder som krävs för att journalföringen fortsättningsvis ska ske på ett lagenligt sätt.

Jag anser att det finns anledning att skicka beslutet till Inspektionen för vård och omsorg (IVO), som är ordinarie tillsynsmyndighet inom hälso- och sjukvårdsområdet, samt till Justitiedepartementet, Socialdepartementet och Sveriges Kommuner och Landsting (SKL) för kännedom.

4.4 Övrigt

Vad som i övrigt har kommit fram leder inte till någon kommentar från min sida.

Ärendet avslutas med den allvarliga kritik mot vårdgivarna som har uttalats.