Hälso- och sjukvårdsnämnden
Stockholms läns landsting
Box 6909
102 39 Stockholm

Tillsyn enligt personuppgiftslagen (1998:204) - samkörning av personuppgifter för gemensam verksamhetsuppföljning

Datainspektionens beslut

Datainspektionen konstaterar att Hälso- och sjukvårdsnämnden i Stockholms läns landsting har

1. behandlat personuppgifter i strid med 2 kap. 4 § patientdatalagen (2008:355) genom att samköra personuppgifter med uppgifter som har samlats in från Vård- och omsorgsnämnden i Österåkers kommun, och

2. överfört personuppgifter via e-post utan att vidta tillräckliga säkerhetsåtgärder enligt i 2 kap. 5 § punkten 2 Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården (SOSFS 2008:14).

Datainspektionen konstaterar att landstingets behandling av personuppgifterna är avslutad och att samtliga personuppgifter som har behandlats är raderade varför inga ytterligare åtgärder vidtas.

Ärendet avslutas.

Redogörelse för tillsynsärendet

Datainspektionen har mottagit ett klagomål rörande en behandling av personuppgifter som har genomförts av Hälso- och sjukvårdsnämnden i Stockholms läns landsting (landstinget) och Vård- och omsorgsnämnden i Österåkers kommun (kommunen). Mot bakgrund av det inkomna klagomålet beslutade Datainspektionen att inleda tillsyn mot landstinget och mot kommunen (beslut dnr 518-2015, bilaga 1).

Bakgrund

Den behandling av personuppgifter som har varit föremål för Datainspektionens granskning genomfördes av kommunen och landstinget som ett led i en nationell satsning på att intensifiera samverkan mellan kommuner och landsting. Syftet med det aktuella projektet var att analysera förutsättningar för ersättningsmodeller som stimulerar till helhetsansvar för vård och omsorg om äldre.

Personuppgiftsbehandlingen som låg till grund för landstingets och kommunens gemensamma verksamhetsuppföljning kan kortfattat beskrivas enligt följande. Landstinget har gjort ett uttag av personuppgifter ur sin VAL-databas och sammanställt ett dataset. Personnumren i dataseten har kodats två gånger med olika hashalgoritmer och salt. Kommunen har på ett liknande sätt gjort ett uttag av personuppgifter ur sin databas ProCapita. Kommunens uppgifter hämtades ur beslut om olika insatser från socialtjänsten. De personnummer som omfattas av kommunens uttag har kodats två gånger med samma hashalgoritmer och salt som landstinget använder. Tieto är personuppgiftsbiträde åt både landstinget och kommunen och sköter driften av VAL-databasen och ProCapita. Tieto har fått i uppdrag av landstinget respektive kommunen att verkställa uttag och kodning av uppgifterna. Tieto har därefter överlämnat landstingets och kommunens separata dataset till landstinget. Landstinget levererade de två dataseten till personuppgiftsbiträdet Nordic Health Group (NHG) som på landstingets uppdrag samkörde och analyserade uppgifterna.

Syftet med Datainspektionens granskning är att kontrollera om det finns legala förutsättningar, enligt rådande lagstiftning, för landsting och kommuner att göra gemensamma verksamhetsuppföljningar som innefattar samkörning av personuppgifter. Datainspektionens beslut utgår ifrån den information som landstinget, muntligen och skriftligen, har lämnat i ärendet.

Det kan noteras att landstingets och kommunens redogörelser för personuppgiftsansvaret och hur personuppgifterna har hanterats inte överrensstämmer på alla punkter.

Landstingets inställning

Landstinget har uppgett i huvudsak följande.

Lagstöd för behandlingen av personuppgifter
Patientdatalagen är tillämplig på den behandling av personuppgifter som har utförts. Ändamålen med behandlingen omfattas av 2 kap. 4 § första stycket 4-6 patientdatalagen. Landstinget menar att det är av intresse för landstingets verksamhet att följa upp hur överlämnandet av patienter till kommunen fungerar. Begreppet ”verksamheten” i punkterna 4-5 i ovan nämnda lagrum omfattar även gemensamma verksamhetsuppföljningar enligt landstingets uppfattning. Den samkörning av landstingets och kommunens personuppgifter som har gjorts är också förenlig med finalitetsprincipen i 9 § första stycket d) personuppgiftslagen (2 kap. 5 § patientdatalagen).

Behandlingen av personuppgifterna m.m.
Personuppgifterna som har analyserats för landstingets räkning har hämtats ur databasen VAL. De variabler som har använts är bland annat personnummer, ålder, kön, in- och utskrivningsdatum, besökstyp, klinik, diagnoskod och remitterande klinik. I VAL-databasen lagras personnummer enbart i form av ett hashat värde. Tieto är personuppgiftsbiträde och sköter driften av VAL-databasen. Det var Tieto som, på uppdrag av landstinget, gjorde urvalet av personuppgifter och sände över datasetet till landstinget med krypterad e-post. Landstinget mottog även ett dataset med personuppgifter från kommunen på samma sätt.

De två separata dataset som landstinget fick från Tieto överlämnades därefter på ett USB-minne till NHG som hade i uppdrag att utföra analysen och bearbetningen av uppgifterna åt landstinget.

Landstinget var personuppgiftsansvarig för den behandling av personuppgifter som Tieto utförde för landstingets räkning. Landstinget menar att kommunen har lämnat ut uppgifter till landstinget genom att Tieto överlämnade kommunens dataset till landstinget. Landstinget anser sig vara ensamt personuppgiftsansvarig för NHG:s samkörning och analys av uppgifterna.

Säkerheten för personuppgifterna
Samtliga personnummer som läggs in i VAL-databasen kodas med en hashalgoritm och ett salt s.k. VAL-krypto. Innan Tieto överlämnade dataseten till landstingen kodades personnumren ytterligare en gång med en ny hashalgoritm och ett salt. För att kunna samköra landstingets uppgifter med kommunens uppgifter, kodade Tieto kommunens urval av personnummer med samma hashalgoritm och salt.

De övriga personuppgifterna som landstinget hämtade ur VAL-databasen utgjorde rådata och gick inte att läsa i klartext utan en översättningstabell. Landstingets inställning är att samtliga uppgifter som har hanterats är personuppgifter men integritetsriskerna för de enskilda individerna bedömdes som små.

Tieto använde programmet Axcrypt för att e-posta de båda dataseten till landstinget. För att få åtkomst till dataseten använde landstinget ett lösenord som skickades av Tieto i ett separat e-postmeddelande.

NHG har destruerat samtliga personuppgifter som överlämnades av landstinget.

Skäl för beslutet

Personuppgifter och personuppgiftsansvar

Landstinget har anfört att de uppgifter som har behandlats är personuppgifter och att landstinget är ensamt personuppgiftsansvarig för de behandlingar som Tieto och NHG har utfört på uppdrag av landstinget.

Enligt 3 § personuppgiftslagen är personuppgifter all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet.

Enligt 2 kap. 6 § patientdatalagen är en vårdgivare personuppgiftsansvarig för den behandling av personuppgifter som vårdgivaren utför.

Skälen för Datainspektionens bedömning är följande
Datainspektionen instämmer i landstingets bedömning att de uppgifter som har bearbetats och analyserats utgör personuppgifter.

Datainspektionen konstaterar att landstinget och kommunen har lämnat motstridiga uppgifter avseende personuppgiftsansvaret för den behandling av personuppgifter som har utförts av NHG. Mot bakgrund bland annat av att den aktuella behandlingen av personuppgifter är avslutad saknar Datainspektionen nödvändiga förutsättningar för att bedöma frågan om personuppgiftsansvarets fördelning. Utgångspunkten i detta beslut är därför att landstinget var ensamt personuppgiftsansvarig för NHG:s samkörning av personuppgifter och för den behandling som utfördes av Tieto på uppdrag av landstinget.

Utlämnande av kodnyckel till kommunen

För att skydda personuppgifterna som behandlas i VAL-databasen lagras samtliga personnummer som ett hashat värde. Kodningen utförs av personuppgiftsbiträdet Tieto som sköter driften av VAL-databasen. Tieto är också personuppgiftsbiträde åt kommunen och sköter driften av kommunens databas ProCapita. För att kunna samköra nämndens och kommunens personuppgifter har Tieto kodat samtliga personnummer från kommunens urval av uppgifter med samma hash och salt som används i VAL-databasen.

Skälen för Datainspektionens bedömning är följande

För att möjliggöra en kodning av kommunens urval av personnummer måste det formellt sett ske ett utlämnande av kodnyckeln från landstinget till kommunen.

Datainspektionen är tillsynsmyndighet enligt personuppgiftslagen och kan inte uttala sig om huruvida det aktuella utlämnandet var förenligt med sekretesslagstiftningen eller inte. Datainspektionen vill emellertid uppmärksamma landstinget på de säkerhetsmässiga risker som kan finnas med att lämna ut en kodnyckel till en utomstående aktör. Kommunen är personuppgiftsansvarig för den kodning av personnummer som Tieto har utfört för kommunens räkning. Kommunen kan inte, som personuppgifts-ansvarig, uppdra åt ett personuppgiftsbiträde att koda personuppgifter utan att kommunen själv har en faktisk möjlighet att ta del av den hashalgoritm och det salt som används. En utlämning av kodnyckeln på det sätt som skett innebär att skyddet för de personuppgifter som behandlas i landstingets VAL-databas riskerar att försämras avsevärt.

Säkerhetsåtgärder vid användning av e-post

Vilken säkerhetsnivå som ska tillämpas vid en vårdgivares hantering av personuppgifter framgår av Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården (SOSFS 2008:14).

Enligt 2 kap. 5 § föreskrifterna ska, om en vårdgivare använder öppna nät för att hantera patientuppgifter, denne ansvara för att det i ledningssystemet finns rutiner som säkerställer att

1. överföringen av patientuppgifter görs på ett sådant sätt att ingen obehörig kan ta del av uppgifterna, och
2. åtkomst till patientuppgifter föregås av stark autentisering.

Skälen för Datainspektionens bedömning är följande
Datainspektionen konstaterar att landstingets överföring av personuppgifter via e-post inte är förenlig med 2 kap. 5 § 2 SOSFS 2008:14 eftersom enbart ett lösenord inte uppfyller kraven på stark autentisering. För att uppnå kraven på stark autentisering krävs att åtkomst till uppgifterna föregås av en autentisering med två faktorer.

Tillåtet ändamål för behandlingen av personuppgifter

En förutsättning för att det ska vara tillåtet för landstinget att samla in och samköra personuppgifter är att behandlingen omfattas av något av de tillåtna ändamålen som anges i 2 kap. 4 § patientdatalagen. Vilka personuppgifter som landstinget får behandla för de ändamål som anges i 2 kap. 4 § regleras i 2 kap. 7 § patientdatalagen.

Landstinget har anfört att den aktuella behandlingen är förenlig med 2 kap. 4 § första stycket 4-6 patientdatalagen. Däri stadgas följande.

Personuppgifter får behandlas inom hälso- och sjukvården om det behövs för

4. att systematiskt och fortlöpande utveckla och säkra kvaliteten i verksamheten,
5. administration, planering, uppföljning, utvärdering och tillsyn av verksamheten, eller
6. att framställa statistik om hälso- och sjukvården.

Av förarbetena till patientdatalagen (prop. 2007/08:126 s. 56) framgår att begreppet ”verksamhet” i 2 kap. 4 § första stycket 4 och 5 syftar på

vårdgivarens egen verksamhet. Bland annat uttalas följande när det gäller regleringen av tillåtna ändamål för personuppgiftsbehandling.

> *Eftersom patientdatalagen får ett väsentligen mera vidsträckt tillämpningsområde i förhållande till vårdregisterlagen är det olämpligt att som idag dela in ändamålen i primära och sekundära ändamål. Både primära och sekundära ändamål handlar om personuppgiftsbehandlingar som, mer eller mindre integrerat, normalt äger rum i varje vårdgivares egen verksamhet.*

När det gäller det specifika ändamålet verksamhetsuppföljning framgår följande av förarbetena till patientdatalagen (a.a. s. 175).

> *Förslagen undanröjer de oklarheter som idag anses gälla i fråga om de rättsliga förutsättningarna för myndigheter inom hälso- och sjukvården och privata vårdgivare att behandla personuppgifter för ändamålet att följa upp sin egen verksamhet. --- När det gäller frågan om att förbättra landstingens och kommunernas möjligheter att göra gemensamma uppföljningar av sådana insatser som involverar både hälso- och sjukvård och socialtjänst så utreds detta för närvarande av Socialtjänstdatautredningen (S2007:92).*

Socialtjänstdatautredningen lämnade i sitt betänkande, Socialtjänsten Integritet – Effektivitet, SOU 2009:32, förslag om att föra in en ny ändamålsbestämmelse i patientdatalagen för att möjliggöra för socialtjänst och hälso- och sjukvården att behandla personuppgifter för gemensamma verksamhetsuppföljningar. Förslaget har emellertid inte lett till vidare lagstiftningsåtgärder.

Landstinget har vidare hänvisat till finalitetsprincipen i 9 § första stycket d) personuppgiftslagen som lagligt stöd för att samköra personuppgifterna.

I förarbetena till patientdatalagen (a.a. s. 60) sägs följande avseende vårdgivares tillämpning av finalitetsprincipen vid behandling av patientuppgifter.

> *[Finalitets]principen hindrar inte att insamlade personuppgifter får behandlas för historiska, statistiska eller vetenskapliga ändamål, eftersom sådana ändamål per definition inte ska anses vara oförenliga med de ursprungliga insamlingsändamålen (9 § andra stycket personuppgiftslagen). Då ändamålsbestämmelserna i patientdatalagen syftar till att vara uttömmande införs i patientdatalagen en uttrycklig hänvisning till dessa bestämmelser i personuppgiftslagen.*

Att ändamålsbestämmelsen i 2 kap 4 § patientdatalagen är uttömmande i förhållande till insamling av personuppgifter framgår också av förarbetena (a.a. s. 56).

> *Patientdatalagens ändamålsreglering blir därmed tydligare och uttömmande i den meningen att vårdgivarna inte själva får besluta om ytterligare ändamål för vilket eller vilka personuppgifter kan samlas in i verksamheten, i vart fall inte utan den registrerades samtycke. Detta är en viktig reglering i integritetshänseende.*

Vidare anges följande (a.a. s. 56 sista stycket).

> *Syftet med ändamålsbestämningen är att ange en yttersta ram för när personuppgifter får samlas in och fortsättningsvis behandlas med stöd av patientdatalagen och personuppgiftslagen.*

Skälen för Datainspektionens bedömning är följande
Datainspektionens konstaterar att landstingets insamling och samkörning av personuppgifter inte omfattas av de tillåtna ändamålen för personuppgifts-behandling i 2 kap. 4 § första stycket 4 och 5 patientdatalagen eftersom behandlingen inte har varit begränsad till landstingets egen verksamhet. Datainspektionen konstaterar vidare att syftet med behandlingen inte primärt var att framställa statistik om hälso- och sjukvården. Behandlingen omfattas därför inte heller av punkten 6 i den aktuella bestämmelsen.

När det gäller finalitetsprincipen har lagstiftaren uttalat att syftet med ändamålsbestämmelsen i 2 kap. 4 § patientdatalagen är att ange en yttersta ram för när personuppgifter får samlas in och fortsättningsvis behandlas med stöd av patientdatalagen och personuppgiftslagen. Vidare uppställer 2 kap. 7 §

patientdatalagen ytterligare begränsningar för insamling och vidarebehandling genom att föreskriva att vårdgivare endast får behandla sådana personuppgifter som behövs för de ändamål som anges i 2 kap. 4 §. Finalitetsprincipen i 9 § första stycket d) personuppgiftslagen, som anger att personuppgifter inte får behandlas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in, ger därför inte landstinget någon annan möjlighet att samla in och bearbeta de personuppgifter som har inhämtats från kommunen.

Datainspektionens slutsats

Landstinget har via sitt personuppgiftsbiträde, NHG, behandlat personuppgifter som har sitt ursprung i en annan verksamhet. Att så har kunnat ske synes ha sin grund i att kommunen och landstinget använder sig av samma personuppgiftsbiträde, Tieto, för att sköta driften av databaserna ProCapita och VAL. Datainspektionen vill betona att ansvaret för en personuppgiftsbehandling åligger den personuppgiftsansvarige även om själva behandlingen utförs av ett personuppgiftsbiträde. Är det frågan om att en verksamhet ska ta del av uppgifter från en annan verksamhet så måste det finnas rättsligt stöd för ett utlämnande och mottagaren måste ha stöd för sin behandling, även om denna sker hos ett personuppgiftsbiträde.

Sammanfattningsvis konstaterar Datainspektionen att det i dagsläget saknas legala förutsättningar för kommuner och landsting, enligt patientdatalagen och personuppgiftslagen, att göra gemensamma verksamhetsuppföljningar på det sätt som skett.

Hur man överklagar

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

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

Katarina Tullstedt

Ingela Alverfors

Bilaga

1. Beslut 518-2015

Kopia till:

1. Socialdepartementet, 103 33 Stockholm
2. Personuppgiftsombudet