LANDSTINGSREVISIONEN

Granskning av landstingets hantering av personuppgifter

Rapport nr 25/2012

VÄSTERBOTTENS LÄNS LANDSTING

Februari 2013

Susanne Hellqvist, revisor, revisionskontoret

Innehåll

1. Sammanfattning

Vi bedömer att landstingsstyrelsen och hälso- och sjukvårdsnämnden inte har en tillfredsställande styrning och uppföljning av att landstinget hanterar personuppgifter enligt gällande lagstiftning. Bedömningen baserar vi på följande iakttagelser:

Ansvarsfördelningen mellan styrelsen och nämnden är inte definierad
Enligt Personuppgiftslagen och Patientdatalagen är varje myndighet i kommuner och landsting personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför. Landstingsfullmäktige fastställer i sitt reglemente för styrelser och nämnder att hälso- och sjukvårdsnämnden leder och samordnar landstingets angelägenheter inom specialistsjukvård, regionsjukvård, tandvård och närsjukvård. Nämnden är enligt reglementet landstingets hälso- och sjukvårdsnämnd enligt hälso- och sjukvårdslagen.

Granskningen visar att ansvarsfördelningen mellan landstingsstyrelsen och hälso- och sjukvårdsnämnden inte är definierad. Det är inte möjligt att utifrån landstingsfullmäktiges säkerhetspolicy avgöra hur personuppgiftsansvaret är fördelat mellan styrelsen och nämnden. Det framgår inte heller av några övriga styrdokument.

En felaktig hantering av personuppgifter kan medföra kränkning av den enskilde och resultera i förtroendeskada och ekonomisk skada för landstinget. Vi anser att det bör vara definierat i vilket avseende respektive nämnd ansvarar för att det finns ett tillfredsställande organisatoriskt och tekniskt skydd för de personuppgifter som verksamheterna hanterar.

Personuppgiftsombudet saknar skriftligt uppdrag
Landstingsdirektören har på uppdrag av landstingsstyrelsen utsett ett personuppgiftsombud för landstinget. Personuppgiftsombudet saknar en skriftlig arbetsbeskrivning som specificerar omfattningen av dennes uppdrag samt vilka nämnder ombudet företräder.

Behov av att se över riktlinjer och hantering
Regler för hur landstingets verksamheter ska gå tillväga vid behandling av personuppgifter finns i 2009 års tryckta regelverk. Reglerna är inte uppdaterade och anpassade till nuvarande organisation. Det finns inga anvisningar på landstingets intranät. Enligt personuppgiftsombudet finns behov av att uppdatera och kommunicera riktlinjer kring vilka behandlingar av personuppgifter som är tillåtna samt vilka behandlingar som landstingets verksamheter ska anmäla till ombudet. Ombudet ser även behov av att göra en inventering över pågående behandlingar och register i verksamheterna för att få överblick över hanteringen. Som exempel lyfter ombudet att denne inte har tillgång till någon förteckning över vilka personuppgiftsbiträdesavtal som landstinget har ingått. Ombudet saknar därmed överblick över vilka externa parter som hanterar personuppgifter för landstingets räkning.

Bristande uppföljning och kontroll
Landstingsstyrelsen och hälso- och sjukvårdsnämnden har inte säkerställt att det finns ett uppföljningssystem som ger nämnderna information om eventuella brister i hanteringen av personuppgifter. Det finns inga dokumenterade rutiner för uppföljning och kontroll av om verksamheterna följer bestämmelser i lagstiftningen. Det före-

kommer ingen återrapportering från personuppgiftsombudet till landstingsstyrelsen, hälso- och sjukvårdsnämnden eller landstingsdirektören.

1.1 Rekommendationer

Vi rekommenderar landstingsstyrelsen och hälso- och sjukvårdsnämnden att:

- Verka för att det blir tydligt definierat hur personuppgiftsansvaret är fördelat mellan styrelsen och nämnden.

- Säkerställa att personuppgiftsombudet får en skriftlig arbetsbeskrivning.

- Säkerställa att det finns dokumenterade riktlinjer för hur landstingets verksamheter ska gå tillväga vid behandling av personuppgifter. Riktlinjerna bör finnas tillgängliga på landstingets intranät.

- Säkerställa en tillfredsställande uppföljning och kontroll av landstingets personuppgiftshantering.

2. Bakgrund

Lagstiftningen ställer krav på att offentliga myndigheter har utvecklade system och en tydlig ansvarsfördelning för hantering av personuppgifter. Syftet med Personuppgiftslagen (PuL) är att skydda den enskilde mot integritetskräkning vid behandling av personuppgifter. Enligt PuL ska en myndighet vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder för att skydda de personuppgifter som myndigheten behandlar.

Brister i hanteringen av personuppgifter kan medföra kränkning av den enskilde och resultera i förtroendeskada och ekonomisk skada för myndigheten.

De förtroendevalda revisorerna genomförde år 2011 en förstudie över hanteringen av personuppgifter i landstingets diarium. Förstudien visade att landstinget saknade riktlinjer för anställdas tillgång till personuppgifter i diariet. I stickprovskontroller kunde revisorerna även notera brister vid registrering av personuppgifter i diariet. Revisorerna har mot bakgrund av iakttagelserna beslutat att år 2012 genomföra en granskning av personuppgiftshanteringen i Västerbottens läns landsting.

2.1 Syfte och revisionsfrågor

Granskningen söker svar på om landstingsstyrelsen och hälso- och sjukvårdsnämnden har en tillfredsställande styrning och uppföljning av att landstinget hanterar personuppgifter enligt gällande lagstiftning.

1) Finns dokumenterade systembeskrivningar på central nivå som tydliggör ansvarsfördelning och befogenheter för hanteringen av personuppgifter?

2) Finns riktlinjer för hur landstingets verksamheter ska gå tillväga vid behandling av personuppgifter?

3) Har styrelsen och nämnden säkerställt en tillräcklig uppföljning och kontroll av hanteringen inom sina respektive verksamhetsområden?

    - Förekommer uppföljning och kontroll av att verksamheterna följer riktlinjer för personuppgiftsbehandling?

    - Finns ett uppföljningssystem som säkerställer att styrelsen och nämnden får information om eventuella brister i hanteringen?

2.2 Avgränsningar

Granskningen avser inte hantering av patientjournaler. Vi har i granskningen inte genomfört några stickprov avseende hanteringen av personuppgifter i landstinget.

Landstingsrevisionen har under hösten 2012 genomfört en granskning av landstingets hantering av patientuppgifter med utgångspunkt av bestämmelser i Patientdatalagen och Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvård (rapport nr 21/2012). Granskningen har varit inriktad på rutiner och kontroller avseende informationssäkerhet för patientuppgifter i landstingets journalsystem SYSteam Cross.

2.3 Revisionskriterier

- Kommunallagen 6 kapitlet § 7
- Landstingsfullmäktiges reglemente för landstingsstyrelsen och hälso- och sjukvårdsnämnden, fastställt 2010-06-01
- Landstingsfullmäktiges säkerhetspolicy, fastställd 2011-06-21
- Patientdatalagen (2008:355)
- Personuppgiftslagen (1998:204)

2.4 Ansvarig styrelse eller nämnd

Vi har i denna granskning avgränsat oss till landstingsstyrelsen och hälso- och sjukvårdsnämnden.

2.5 Metod och genomförande

Granskningen baseras på dokumentstudier och intervjuer med landstingets personuppgiftsombud vid staben för planering och styrning. Ombudet har getts möjlighet att lämna synpunkter på rapportens innehåll. Rapporten har även kvalitetssäkrats genom att den granskats av annan sakkunnig vid revisionskontoret.

3. Landstingets hantering av personuppgifter

3.1 Om personuppgifter

Med personuppgifter avses enligt Personuppgiftslagen all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet.

Med behandling av personuppgifter avses varje åtgärd eller serie av åtgärder som vidtas i fråga om personuppgifter, exempelvis insamling, registrering, utlämnande, spridning, sammanställning och samkörning.

3.2 Lagstiftningens krav på hantering av personuppgifter

Hur ett landsting ska hantera personuppgifter finns reglerat i Patientdatalagen och Personuppgiftslagen (PuL).

Syftet med Personuppgiftslagen är att skydda den personliga integriteten vid behandling av personuppgifter som är helt eller delvis automatiserad. Lagen är även tillämplig på viss manuell behandlig av personuppgifter, om personuppgifterna ingår i en strukturerad samling av uppgifter som är tillgänglig för sökning eller sammanställning. Om det finns bestämmelser i andra lagar som avviker från Personuppgiftslagen gäller dessa före Personuppgiftslagen.

Patientdatalagen är tillämplig vid en vårdgivares behandling av personuppgifter inom hälso- och sjukvården. Lagen kompletterar och går i vissa avseenden före bestämmelser i Personuppgiftslagen. I Patientdatalagen finns preciserat vad som gäller vid behandling av personuppgifter i regionala och nationella kvalitetsregister. I lagen finns också bestämmelser om vårdgivares skyldighet att föra patientjournal.

Statlig tillsynsmyndighet för hantering av personuppgifter är Datainspektionen.

3.3 Ansvarsfördelning enligt lagstiftningen

I Patientdatalagen och Personuppgiftslagen finns följande bestämmelser avseende ansvarsfördelningen för hantering av personuppgifter:

Personuppgiftsansvar: Personuppgiftsansvarig är enligt Personuppgiftslagen den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter. Enligt uppgift på Datainspektionens webbplats ligger personuppgiftsansvaret i en kommun hos de kommunala nämnder som är så pass självständiga att de är förvaltningsmyndigheter. Den personuppgiftsansvarige ska enligt Personuppgiftslagen vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som myndigheten behandlar.

Av Patientdatalagen framgår att varje myndighet inom kommuner och landsting som bedriver hälso- och sjukvård är personuppgiftsansvarig för verksamhetens behandling av personuppgifter: ”*I landsting och kommun är varje myndighet som bedriver hälso- och sjukvård personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför”(2 kap. 6 §)*.

Personuppgiftsansvaret är straff- och skadeståndssanktionerat.

Personuppgiftsombud: Ett personuppgiftsombud är en fysisk person som efter förordnande från den personuppgiftsansvarige självständigt ska se till att verksamheten behandlar personuppgifter på ett korrekt och lagligt sätt. Ett personuppgiftsombud kan representera flera personuppgiftsansvariga.

Enligt Personuppgiftslagen ska den som är personuppgiftsansvarig anmäla automatiserade behandlingar av personuppgifter till Datainspektionen. Det finns dock undantag från anmälningsskyldigheten. Behandlingar som regleras av föreskrifter i annan lag eller förordning, exempelvis Patientdatalagen, omfattas inte av anmälningsskyldigheten. Den personuppgiftsansvarige behöver inte heller anmäla behandlingar som omfattas av anmälningsskyldigheten till Datainspektionen om den ansvarige har utsett ett personuppgiftsombud. Det är i sådana fall tillräckligt att den ansvarige anmäler behandlingen till ombudet som kontrollerar lagligheten i denna. Personuppgiftsombudet ansvarar för att föra en förteckning över anmälda behandlingar för den personuppgiftsansvariges räkning.

Personuppgiftsbiträde: Ett personuppgiftsbiträde är en extern part som behandlar personuppgifter på uppdrag av den personuppgiftsansvarige. Det ska finnas ett skriftligt avtal om personuppgiftsbiträdets behandling av personuppgifter för den personuppgiftsansvariges räkning. När den personuppgiftsansvarige anlitar ett biträde ska den personuppgiftsansvarige förvissa sig om att biträdet kan vidta lämpliga säkerhetsåtgärder och säkerställa till att biträdet verkligen gör det.

3.4 Ansvarsfördelning i Västerbottens läns landsting

Landstingsfullmäktige fastställde i juni 2011 en säkerhetspolicy för Västerbottens läns landsting. Det finns inga anvisningar i policyn avseende personuppgiftsansvar och organisation för hantering av personuppgifter i landstinget.

Landstingsstyrelsen har beslutat om en ”Strategi för säkerhet och beredskap”. I riktlinjerna fastställer landstingsstyrelsen att landstingsdirektören har det övergripande ansvaret för informationssäkerheten i landstinget. I detta uppdrag ligger enligt styrelsen att direktören ska utforma övergripande bestämmelser för informationssäkerhet samt vara personuppgiftsombud för landstinget.

Landstingsdirektören har fastställt riktlinjer för informationssäkerhet i september 2011. Landstingsdirektören har därutöver i april 2012 utsett en av landstingets jurister vid staben för planering och styrning till personuppgiftsombud och anmält förordnandet till Datainspektionen. Av anmälan till Datainspektionen framgår att personuppgiftsombudet är ombud för Västerbottens läns landsting.

Personuppgiftsombudet har enligt uppgift ingen skriftlig arbetsbeskrivning som specificerar vad uppdraget består i och vilka nämnder som ombudet är företrädare för.

3.5 Vår kommentar

Enligt Personuppgiftslagen och Patientdatalagen är varje myndighet i kommuner och landsting personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför. Landstingsfullmäktige fastställer i sitt reglemente för styrelser och nämnder att hälso- och sjukvårdsnämnden leder och samordnar landstingets angelägenheter inom specialistsjukvård, regionsjukvård, tandvård och närsjukvård.

Nämnden är enligt reglementet landstingets hälso- och sjukvårdsnämnd enligt hälso- och sjukvårdslagen.

Granskningen visar att ansvarsfördelningen mellan landstingsstyrelsen och hälso- och sjukvårdsnämnden inte är definierad. Det är inte möjligt att utifrån landstingsfullmäktiges säkerhetspolicy avgöra hur personuppgiftsansvaret är fördelat mellan styrelsen och nämnden. Det framgår inte heller av några övriga styrdokument.

En felaktig hantering av personuppgifter kan medföra kränkning av den enskilde och resultera i förtroendeskada och ekonomisk skada för landstinget. Vi anser att det bör vara definierat i vilket avseende respektive nämnd ansvarar för att det finns ett tillfredsställande organisatoriskt och tekniskt skydd för de personuppgifter som verksamheterna hanterar.

3.6 Riktlinjer till verksamheterna

Det finns inga riktlinjer eller anvisningar på landstingets intranät för hur landstingets verksamheter ska gå tillväga vid behandling av personuppgifter.

I landstingets tryckta regelverk från år 2009 finns under kapitlet ”IT” ett avsnitt med information kring lagstiftningen på området samt grundläggande regler vid behandling av personuppgifter. Regelverket är sedan maj 2012 inte tillgängligt på landstingets intranät. Av det tryckta regelverket framgår att verksamheterna ska anmäla all behandling av personuppgifter som är helt eller delvis automatiserad till landstingets personuppgiftsombud. Anmälan ska verksamheten göra på en särskild blankett. När regelverket fanns tillgängligt på intranätet fanns en länk till blanketten. I regelverket finns hänvisning till en person som tidigare innehade funktionen som personuppgiftsombud.

Landstingets nuvarande personuppgiftsombud tog i april 2012 över uppgiften från ett tidigare utsett ombud vid informatikenheten. Av intervjuer framkommer att personuppgiftsombudet hanterar anmälningar från verksamheterna manuellt. Blanketterna med anmälda behandlingar finns samlade i en pärm som är sorterad efter anmälningsår. Antalet anmälningar under åren 2008-2012 uppgår till 1-3 stycken årligen.

Enligt personuppgiftsombudet finns behov av att uppdatera och kommunicera riktlinjer kring vilka behandlingar av personuppgifter som är tillåtna samt vilka behandlingar som landstingets verksamheter ska anmäla till ombudet. Ombudet ser även behov av att göra en inventering över pågående behandlingar och register i verksamheterna för att få överblick över hanteringen. Som exempel lyfter ombudet att denne inte har tillgång till någon förteckning över vilka personuppgiftsbiträdesavtal som landstinget har ingått. Ombudet saknar därmed överblick över vilka externa parter som hanterar personuppgifter för landstingets räkning.

3.7 Uppföljning och kontroll

Enligt Personuppgiftslagen ska den som är utsedd till personuppgiftsombud påpeka brister för den personuppgiftsansvarige om det finns risk för att verksamheten bryter mot bestämmelser i lagstiftningen. Om den personuppgiftsansvarige inte vidtar åtgärder ska personuppgiftsombudet anmäla förhållandet till Datainspektionen.

Det finns inga krav i lagstiftningen på att personuppgiftsombudet ska genomföra regelbundna kontroller eller revisioner av att verksamheten följer lagstiftningen för hantering av personuppgifter. Datainspektionen rekommenderar i tillämpningsanvisningar för personuppgiftsombud att ombudet i sitt arbete bör utgå från dokumenterade rutiner för hur tillsynen ska gå till.

Enligt uppgift från personuppgiftsombudet finns inga dokumenterade direktiv från landstingsstyrelsen, hälso- och sjukvårdsnämnden eller landstingsdirektören till denne att genomföra kontroller av hanteringen av personuppgifter. Det förekommer ingen återrapportering från personuppgiftsombudet till landstingsdirektör eller nämnder. Personuppgiftsombudets arbete består i att ge stöd och råd på begäran av verksamheterna, att bistå vid upprättande av personuppgiftsbiträdesavtal samt att kontrollera lagligheten i behandlingar när verksamheter anmäler sådana.

3.8 Svar på revisionsfrågor

Revisionsfråga	**Bedömning**
Finns dokumenterade systembeskrivningar på central nivå som tydliggör ansvarsfördelning och befogenheter för hanteringen av personuppgifter?	Delvis. Det är inte definierat hur personuppgiftsansvaret är fördelat mellan hälso- och sjukvårdsnämnden och landstingsstyrelsen. Landstingsdirektören har beslutat om en informationssäkerhetspolicy. Det finns ett utsett personuppgiftsombud. Ombudet saknar dock en skriftlig arbetsbeskrivning.
Finns riktlinjer för hur landstingets verksamheter ska gå tillväga vid behandling av personuppgifter?	Delvis. Regler finns i 2009 års tryckta regelverk. Reglerna är dock inte uppdaterade och anpassade till nuvarande organisation. Det finns inga riktlinjer på landstingets intranät.
Förekommer uppföljning och kontroll av att verksamheterna följer riktlinjer för personuppgiftsbehandling?	Nej.
Finns ett uppföljningssystem som säkerställer att styrelsen och nämnden får information om eventuella brister i hanteringen?	Nej.

Umeå den 21 februari 2013

Susanne Hellqvist
Revisor