Revisionsrapport

# *Granskning, efterlevnad av Patientdatalagen (2008:355)*

## *Landstinget i Värmland*

*Eva Lidmark,*
*Magnus Olson-Sjölander*

*20 december 2011*

# *Innehållsförteckning*

# 1 Sammanfattning

PwC har av revisorerna i Landstinget i Värmland fått i uppdrag att granska efterlevnad av Patientdatalagen (2008:355) med tillhörande föreskrift om informationshantering och journalföring i hälso- och sjukvården (SOSFS 2008:14).

Patientdatalagen (PDL) trädde i kraft den 1 juli 2008 och innehåller en samlad reglering av informationshanteringen inom hälso- och sjukvården. Lagen ersätter Lag om vårdregister (1998:544) och Patientjournallagen (1985:562) och ska tillämpas av alla vårdgivare, både i privat och i offentlig regi. Syfte med lagen är att informationshantering inom hälso- och sjukvården ska vara organiserad så att den tillgodoser patientsäkerhet, patientnytta och god kvalitet samt främjar kostnadseffektivitet. Personuppgifter ska utformas och i övrigt behandlas så att patienters och övriga registrerades integritet respekteras. Precis som idag ska personuppgifter hanteras och förvaras så att obehöriga inte får tillgång till dem.

De revisionsfrågor som revisorerna önskar få besvarade är följande:
*– Har landstingsstyrelsen genom styrning, uppföljning och intern kontroll säkerställt att landstinget efterlever gällande bestämmelser?*
*– Efterlever Landstinget i Värmland Patientdatalagen med tillhörande föreskrift?*
*– Om det finns brister i styrning, uppföljning och intern kontroll respektive efterlevnad av lagen, vilka förbättringsåtgärder behöver vidtas?*

**Granskningen visar att**:

Landstingsstyrelsen har utsett en informationssäkerhetsansvarig. Därtill finns en rad funktioner och grupperingar som på olika sätt arbetar med frågor som relaterar till informationssäkerhet.

**Vi bedömer att:**

- det finns brister i tydlighet mellan dessa funktioner och grupperingar sett till uppdrag, ansvar och avgränsningar dem emellan
- gruppernas sammansättning inte säkerställer att informationssäkerhetsperspektivet fullt ut beaktas
- uppföljning av funktionernas och gruppernas arbete inte är tillfredsställande
- det är en stor brist att landstingsstyrelsen inte gett direktiv om och säkerställt att landstinget har en informationssäkerhetspolicy
- det med dagens arbetssätt, finns brister i informationsflödet mellan informationssäkerhetsansvarig och vårdgivaren
- det är en brist för landstingets arbete med informationssäkerhet att ett ledningssystem för kvalitet och patientsäkerhet ännu inte är implementerat

- det är en brist att det i landstinget inte finns någon samlad bild av vilka vårdinformationssystem som innehåller patientuppgifter
- det finns oklarheter i ansvarsfrågor avseende informationssäkerheten då det inte finns någon dokumentation som tydligt beskriver vilket ansvar vårdgivaren lagt på verksamhetschefen
- det inte går att säkerställa att landstingsstyrelsen lever upp till Patientdatalagens och föreskrift 2008:14 krav på behörighetstilldelning för samtliga vårdinformationssystem
- det är en brist att det inte gjorts någon behovs- och riskanalys på de behörigheter som används i Cosmic PAS, ett av landstingets mest centrala vårdsystem
- landstingsstyrelsen inte säkerställt Patientdatalagens och föreskrift 2008:14 krav på spärrhantering
- övergripande regelverk vid logguppföljning är framtaget vilket är tillfredsställande. Däremot framgår det inte i regelverket vad som gäller för logguppföljning för övriga vårdinformationssystem annat än för landstingens journalsystem
- rutinen för journalföring och hantering av åtkomst till patientuppgifter inte är tillfredsställande i de delar som avser att dokumentation ska vara åtkomlig och användbar utan fördröjning för den som är behörig
- landstinget har ett avvikelsehanteringssystem vilket är tillfredsställande. Däremot går det inte att få ut statistik som visar på avvikelser relaterade till Patientdatalagen och/eller föreskrift 2008:14
- den riktade utbildningsinsatsen för läkarsekreterare samt den generella utbildning som samtliga verksamhetschefer genomgår är tillfredsställande. Däremot saknas riktade utbildningsinsatser för Patientdatalagen och föreskrift 2008:14 som når samtlig personal.

**Vår samlade bedömning** är att landstingsstyrelsen, pga. brister i styrning, uppföljning och intern kontroll, inte säkerställer att landstinget efterlever gällande bestämmelser. Det innebär att Landstinget i Värmland endast i ett fåtal delar efterlever Patientdatalagen och föreskrift 2008:14. Sammanställning på förslag på förbättringsåtgärder lämnas i avsnitt 4.

# 2 Inledning

## 2.1 Utgångspunkt för granskningen

Patientdatalagen (PDL) trädde i kraft den 1 juli 2008 och innehåller en samlad reglering av informationshanteringen inom hälso- och sjukvården. Lagen ersätter Lag om vårdregister (1998:544) och Patientjournallagen (1985:562) och skall tillämpas av alla vårdgivare, både i privat och i offentlig regi. Förarbete till lagen framgår av prop. 2007/08:126. I sekretesslagen (1980:100) införs samtidigt förändringar föranledda av PDL samt ytterligare ändringar avsedda att stärka patientsäkerheten. Vidare har Socialstyrelsen utkommit med föreskrift om informationshantering och journalföring i hälso- och sjukvården 2008:14. Slutligen har också Sveriges Kommuner och Landsting (SKL) utarbetat information som publicerats i cirkulär 08:55. Personuppgiftslagen (1988:204) är subsidiär[1] i förhållande till PDL och gäller om inte annat följer av PDL eller föreskrifter som meddelats med stöd av PDL.

Lagens syfte är att informationshantering inom hälso- och sjukvården ska vara organiserad så att den tillgodoser patientsäkerhet, patientnytta och god kvalitet. Lagen ska även främja kostnadseffektivitet, att personuppgifter utformas och i övrigt behandlas så att patienters och övriga registrerades integritet respekteras.

PDL ska tillämpas vid behandling av personuppgifter i alla vårdgivares kärnverksamhet som avser tillhandahållande av hälso- och sjukvård inklusive tandvård åt patienter.

PDL ska också tillämpas på dokumentation m.m. i patientjournaler (3 kap). Dessa bestämmelser är tillämpliga även om behandlingen sker manuellt utan att personuppgifterna ingår i eller avses ingå i någon strukturerad uppgiftssamling.

Tillämpningsområdet omfattar all helt eller delvis automatiserad behandling av personuppgifter samt manuell behandling av personuppgifter som ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier. Regleringen är således inte begränsad till särskilda datoriserade register, databaser eller andra elektroniska uppgiftssamlingar.

I PDL är begreppet sammanhållen journalföring infört. Definitionen är ”Ett elektroniskt system”, som gör det möjligt för en vårdgivare att ge eller få åtkomst till personuppgifter hos en annan vårdgivare (1 kap 3 §). Det finns även en regel om inre sekretess införd(4 kap 1 §), att vårdgivarna åläggs begränsa personalens åtkomst till patientuppgifter till vad som behövs för att den enskilde (personal) ska kunna utföra sina arbetsuppgifter inom hälso- och sjukvården (4 kap 2 §) samt kontrollera elektronisk åtkomst (4 kap 3 §).

[1] understödjande

Landstingets revisorer ansvarar för att genomföra årlig granskning av landstingets samtliga verksamheter. I revisorernas riskbedömning och revisionsplan för 2011 ingår en granskning av landstingets patientsäkerhetsarbete.

Detta uppdrag avser granskning av efterlevnad av Patientdatalagen (2008:355) med tillhörande föreskrifter. Den föreskrift som granskningen tar sin utgångspunkt i är Socialstyrelsens föreskrift om informationshantering och journalföring i hälso- och sjukvården (SOSFS 2008:14).

## 2.2 Uppdrag och revisionsfrågor

PwC har av revisorerna i Landstinget i Värmland fått i uppdrag att granska efterlevnad av patientdatalagen med tillhörande föreskrifter. De revisionsfrågor som revisorerna önskar få besvarade är:

- *Har landstingsstyrelsen genom styrning, uppföljning och intern kontroll säkerställt att landstinget efterlever gällande bestämmelser?*
- *Efterlever Landstinget i Värmland patientdatalagen med tillhörande föreskrifter?*
- *Om det finns brister i styrning, uppföljning och intern kontroll respektive efterlevnad av lagen, vilka förbättringsåtgärder behöver vidtas?*

## 2.3 Metod och genomförande

Granskningen har genomförts genom intervjuer med:

- landstingets hälso- och sjukvårdschef
- chefläkare och tillika processägare patientsäkerhet
- verksamhetschef och medarbetare från njurmedicinska kliniken
- biträdande verksamhetschef och medarbetare från kirurgkliniken
- verksamhetschef vårdadministrativ enhet
- informationssäkerhetsansvarig
- landstingsarkivarie tillika personuppgiftsombud
- landstingets jurist samt
- systemägare för journalsystem COSMIC.

Granskning har skett av dokumentation som har tillhandahållits av intervjupersonerna.

Rapporten har sakgranskats av intervjupersonerna under vecka 50.

# 3 Granskningsresultat

## 3.1 Övergripande säkerhetsstyrning

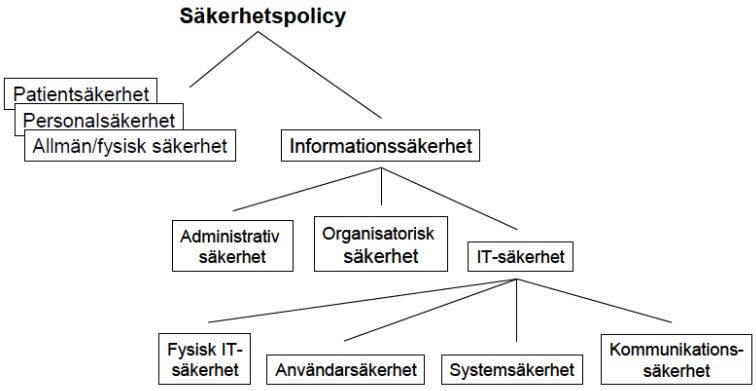
*Inom detta område granskas den övergripande säkerhetsstyrningen med fokus på organisation, processer och flöden.*

### 3.1.1 Iakttagelser

Informationssäkerhet är en patientsäkerhetsfråga under vårdgivarens ansvar. Informationssäkerheten ska ingå som en del av vårdgivarens ledningssystem för kvalitet och patientsäkerhet[2]. Arbetet med att ta fram ett ledningssystem pågår.

Ansvaret för informationssäkerheten beskrivs på följande sätt i dokument *Delegation till informationssäkerhetsansvarig*[3]. ”Landstingsdirektören har ett övergripande uppdrag och ansvar inom säkerhetsområdet med avseende på bl. a ledning, samordning, planering, uppföljning och utvärdering. Arbetsområdet kan beskrivas utifrån fyra perspektiv – patient-, personal-, allmän/fysisk- samt informationssäkerhet”.

I dokumentet beskrivs informationssäkerhetsområdet med följande figur:




Någon säkerhetspolicy (enligt bilden ovan) finns inte, däremot ett *Säkerhetsprogram för Landstinget i Värmland*, antaget av landstingsstyrelsen[4]. I dokumentet refereras till en landstingsövergripande säkerhetskommitté. Enligt intervjupersonerna är denna kommitté inte aktiv i dagsläget utan kommer att få ett annat utseende. Hälso- och sjukvårdschefen menar att det behövs nya och bättre forum för vårdsäkerhet (inom vilken informationssäkerheten är en del)där informationssäkerhetsansvarig deltar.

[2] SOSFS 2005:12
[3] Dnr LK/070068
[4] Antaget den 8 juni 2004

Landstingsdirektören har sedan 2007 överfört ansvaret för arbetsuppgifter inom informationssäkerhetsområdet till landstingets informationssäkerhetsansvarige. Informationssäkerhetsansvarig är organisatoriskt placerad i den administrativa staben inom landstingets kansli. Arbetsuppgifter och befogenheter innebär bland annat att övergripande leda och utveckla det koncernövergripande informationssäkerhetsarbetet.

I informationssäkerhetsansvariges uppdrag ligger att regelbundet informera landstingsdirektören om läge och utveckling. Det finns ingen formell form för denna information. I förekommande fall går information från informationssäkerhetsansvarig till landstingsdirektören i linjen vilket innebär tre mellanchefer mellan informationssäkerhetsansvarig och landstingsdirektören. Det innebär att informationssäkerhetsansvarig inte själv är föredragande vilket upplevs som en brist av vederbörande.

Informationssäkerhetsrapport 2010 för landstinget i Värmland är framtagen och redovisad för landstingsstyrelsen mer som ett informationsärende med förklarande åtgärder från landstingsdirektörens ledningsgrupp.

Fr.o.m. den 1/1 2012 kommer informationssäkerhetsansvarig organisatoriskt att tillhöra landstings-IT. Denna förändring är föranledd av en organisationsöversyn[5]. I den aktuella rapporten[6] framgår att ett motiv till denna organisatoriska förändring är att informationssäkerhetsarbetet i stor utsträckning är tätt sammankopplat med IT-frågorna. I rapporten anges att genom denna förändring kan en naturlig koppling till inte bara IT-säkerheten utan även övrig kompetens kring arkitektur och strategier inom IT-området uppnås.

I landstinget finns en strategisk grupp för informationshantering (SGI) som leds av informationssäkerhetsansvarig. SGI etablerades samtidigt som funktionen informationssäkerhetsansvarig dvs. 2007. Gruppen fungerar bra men det är oklart på vems uppdrag gruppen arbetar i dagsläget och vilket mandat den har. En annan brist är att den saknar koppling till andra forum som arbetar med patientsäkerhetsrelaterade frågor. I SGI ingår, förutom informationssäkerhetsansvarig, även IT-säkerhetsansvarig, personuppgiftsombud/landstingsarkivarie, företrädare för medicinsk teknik, chef för läkarsekreterarna samt landstingsjuristen. Gruppen har nyligen kompletterats med en verksamhetschef för vårdadministration för att säkra verksamhetsperspektivet i gruppens arbete. Däremot ingår inte chefläkaren, tillika processägare för patientsäkerhet, i denna grupp.

Grupperingen Klinisk Beslutsgrupp Vårdsystem (KBV) ska ses som Hälso- och sjukvårdsledningens och Styrgrupp Vårdsystems operativa beslutsfattande del för att omvandla övergripande beslut till detaljoperativ funktion rörande vårdsystem. Praktiskt är KBV underställd Styrgrupp Vårdsystem och i sig hälso- och sjukvårdschefen. Ordförande i KBV återrapporterar ca 3 ggr per termin direkt till

[5] Daterat 2011-08-11, LK/111442
[6] IT-verksamheten inom LiV 2012, LK111/442

hälso- och sjukvårdschefen. Informationssäkerhetsansvarig finns inte med i denna grupp.

KBV's uppdrag beskrivs på följande sätt[7]:

- ansvara för operativa beslut rörande LiV:s samtliga vårdsystem som ligger utanför direkt IT-förvaltning och i de fall inte uttalad systemförvaltningsgrupp och systemägare redan hanterar sådana frågor. Även i dessa fall skall KBV informeras och ge synpunkter på alla frågor som rör beslut om integration mellan system, samt sådana frågor som påverkar, direkt eller indirekt, sådan integration.

- agera utifrån LiV:s övergripande IT-strategi att COSMIC är landstingets sammanhållande och viktigaste vårdsystem som om möjligt ska vara datakälla för vårdinformationen i LiV. KBV skall också uttryckligen fungera som beslutsgrupp för konfigurering, strategiska vägval och inriktning av COSMIC i LiV. Löpande återföring från COSMIC förvaltning och eventuella andra COSMIC projekt skall ske till KBV.

- ha ett regionalt och nationellt perspektiv i sin beredning av olika frågor så att man om möjligt ansluter till lösningar som också andra landsting och organisationer använder samt säkerställa att LiV:s behov av uppföljning på olika nivåer ur Vårdsystem kan uppfyllas.

- genom ordföranden ha förankrat ekonomiska konsekvenser av beslut i LiV:s linjeorganisation innan definitiva beslut tas. KBV har inget eget budgetansvar.

- hantera avvikelser rörande vårdsystem som rör systemövergripande aspekter eller driftstörningar, säkerhet mm.

- ha patientsäkerhets- och arbetsmiljöfokus i all sin verksamhet och i lösningar också beakta användarvänlighet och ha patientfokus för att minimera administration och maximera flödet genom vårdprocesserna.

Det finns i landstinget ingen samlad förteckning av vilka vårdinformationssystem som innehåller patientuppgifter. Enligt uppgift rör det sig ett okänt antal system där 23 är kartlagda avseende vissa krav i patientdatalagen.

### *3.1.2 Bedömning*

- Landstingsstyrelsen har utsett en informationssäkerhetsansvarig. Därtill finns en rad funktioner och grupperingar som på olika sätt arbetar med frågor som relaterar till informationssäkerhet.

- Vi bedömer att det finns brister i tydlighet mellan dessa funktioner och grupperingar sett till uppdrag, ansvar och avgränsningar dem emellan.

[7] Daterat 110118, enligt dokumentet diskuterat med Hälso- och sjukvårdschef Gunilla Andersson och förelagt Hälso- och sjukvårdsledningen januari 2011

Vidare bedömer vi att gruppernas sammansättning inte säkerställer att informationssäkerhetsperspektivet fullt ut beaktas. Vi bedömer också att uppföljning av funktionernas och gruppernas arbete inte är tillfredsställande.

- Vi bedömer att det, med dagens arbetssätt, finns brister i informationsflödet mellan informationssäkerhetsansvarig och vårdgivaren.

- Vi bedömer att det är en brist för landstingets informationssäkerhetsarbete att ett ledningssystem för kvalitet och patientsäkerhet ännu inte är fullt implementerat.

- Vi bedömer det vara en brist att det i landstinget inte finns någon samlad bild av vilka vårdinformationssystem som innehåller patientuppgifter. En samlad bild är en förutsättning för att säkerställa att Patientdatalagen och föreskriften efterlevs.

**Förslag till åtgärder:**

- Tydliggör roller, ansvar, avgränsningar mellan de olika funktioner och grupperingar som arbetar med frågor som relaterar till PDL och föreskriften. Beskriv och kommunicera mandat, syfte och sammanhang för samtliga funktioner och grupperingar. Säkerställ att grupperna företräds av funktioner som bidrar till gruppens förväntade effekt.

- Säkerställ att informationssäkerhetsansvarigs organisatoriska tillhörighet till Landstings-IT *inte* innebär att ansvaret att styra och ställa krav på informationssäkerheten läggs på IT-avdelningen. En IT-avdelning ska leverera det kravställaren begär, de kan inte ta över ansvaret för risker som rör patientsäkerheten. Informationssäkerhet är en patientsäkerhetsfråga under vårdgivarens ansvar och ska ingå som en del av vårdgivarens ledningssystem för kvalitet och patientsäkerhet.

- Upprätta en samlad förteckning av vilka vårdinformationssystem som innehåller patientuppgifter och i vilken utsträckning de möter kraven i Patientdatalagen och föreskrift 2008:14.

## 3.2 Roller och ansvar

*Inom detta område granskas roller och ansvar som finns inom organisationen för att efterleva lagar och föreskrifter.*

### 3.2.1 Iakttagelser

Landstingsjuristen har ingen uppdragsbeskrivning där dennes uppdrag i arbetet med att säkerställa efterlevnad av Patientdatalag och tillhörande föreskrifter framgår. Ett generellt arbete pågår med att kartlägga och tydliggöra en struktur för vårdgivarens ansvar och vilka direktiv vårdgivaren måste ge utifrån lagar och föreskrifter. Idag finns ingen struktur för detta, inte heller en struktur för att föra ut landstingsstyrelsens direktiv och beslut ut i organisationen på underliggande ansvarsnivåer.

Chefläkaren är tillika processägare patientsäkerhet. Detta uppdrag omfattar, sedan 1/9 2011, 100 %. Det finns i dagsläget ingen uppdragsbeskrivning där chefläkarens uppdrag i arbetet med att säkerställa efterlevnad av patientdatalag och tillhörande föreskrifter framgår. Det finns inte heller någon etablerad samverkan mellan denna funktion och informationssäkerhetsansvarig.

Föreskriften 2008:14 anger att vårdgivaren ska se till att informationshanteringen inom hälso- och sjukvården tillgodoser patientsäkerhet, håller hög kvalitet samt främjar kostnadseffektivitet. I detta ansvar ingår att utse verksamhetschefer som inom ramen för ledningssystemet ska ta fram, fastställa och dokumentera ändamålsenliga rutiner för informationshanteringen. Det ska finnas en skriftlig dokumentation som tydligt beskriver vilket ansvar vårdgivaren har lagt på verksamhetschefen. En sådan dokumentation finns inte i landstinget.

### *3.2.2 Bedömning*

- Vi bedömer att det finns oklarheter i ansvarsfrågor avseende informationssäkerheten då det inte finns någon dokumentation som tydligt beskriver vilket ansvar vårdgivaren lagt på verksamhetschefen.

- Se vidare våra bedömningar ovan under punkt 3.1.2.

**Förslag till åtgärder:**

- Ta fram skriftlig dokumentation som tydligt beskriver vilket ansvar vårdgivaren har lagt på verksamhetschefen sett till informationshantering.

- Säkerställ att verksamhetscheferna tar fram, fastställer och dokumenterar ändamålsenliga rutiner för informationshanteringen.

- Se vidare våra förslag till åtgärder ovan under punkt 3.1.2.

## *3.3 Informations-/IT-säkerhetspolicy*

*Inom detta område är de styrande dokumenten centrala, såväl utformning som innehåll och tillämpning granskas.*

### *3.3.1 Iakttagelser*

Enligt föreskriften 2008:14 ska vårdgivaren ge direktiv och säkerställa att det i verksamhetens ledningssystem för kvalitet och patientsäkerhet finns en dokumenterad informationssäkerhetspolicy. Ett sådant direktiv är inte givet och det finns inte heller någon informationssäkerhetspolicy framtagen. I intervjuerna hänvisas istället till *Informationssäkerhetshandboken*.

*Informationssäkerhetshandboken* är ett omfattande dokument på knappt 200 sidor. Ett mindre omfattande dokument är *Lilla informationssäkerhetshandboken* som är en förkortad version av *Informationssäkerhetshandboken*. *Informationssäkerhetshandboken* är från 2001 och är inte reviderad i samband

med Patientdatalagens och föreskrift 2008:14 ikraftträdande. I denna handbok berörs inte heller något om Personuppgiftslagen.

Informationssäkerhetsansvarig inväntar vårdgivarens direktiv om framtagande av en informationssäkerhetspolicy. Vid ett möte med teknikutskottet i maj 2011 uppmärksammade informationssäkerhetsansvarig ledamöterna på behov av vårdgivardirektiv i denna fråga. Informationssäkerhetsansvarig räknar med att detta direktiv kommer under 2012 och att policyn kommer att tas fram under samma år.

### 3.3.2 Bedömning

- En informationssäkerhetspolicy är en grundläggande förutsättning för att kunna säkerställa efterlevnad till PDL och föreskrift 2008:14. En informationssäkerhetspolicy ska vara tydlig och kortfattad så att all personal ska kunna ta den till sig. En handbok är ett av de dokument som har informationssäkerhetspolicyn som grund.

- Det är en stor brist att landstingsstyrelsen inte gett direktiv om och säkerställt att landstinget har en informationssäkerhetspolicy.

- Vi bedömer att det är en brist att informationssäkerhetshandboken inte är reviderad sedan 2001.

**Förslag till åtgärder:**

- Ge direktiv om ta fram en informationssäkerhetspolicy och prioritera arbetet med att ta fram en sådan. Skapa en rutin för att kontinuerlig följa upp och revidera denna policy.

- Revidera *Informationshandboken*. Säkerställ att *Informationshandboken* beaktar Personuppgiftslagen. Skapa en rutin för att kontinuerlig följa upp och revidera denna handbok.

- Säkerställ att anställda informeras om och utbildas i dessa dokument.

## 3.4 Behörigheter och åtkomst

*Inom detta område granskas rutiner för behörigheter och åtkomst, såväl processer som vissa system granskas. Delområden som omfattas är signering, spärrning och säkerhetskopiering av patientuppgifter.*

### 3.4.1 Iakttagelser

Vad gäller behörighetstilldelning anges i 4 kap. 2 § Patientdatalagen att vårdgivaren ska begränsa en användares behörigheter till vad som behövs för att användaren ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården. Bestämmelsen kompletteras sedan av 2 kap. 6 § SOSFS 2008:14, där det bl.a. framgår att varje användare ska tilldelas en individuell behörighet och att vårdgivarens beslut om tilldelning av behörighet ska föregås av en behovs- och riskanalys. Enligt samma

föreskrift ska vårdgivaren även ansvara för att det finns rutiner för tilldelning, förändring, borttagning och regelbunden uppföljning av behörigheterna.

Vad gäller styrande dokument relaterat behörighetstilldelning hänvisas i intervjuer till dokument *Riktlinje för tillgång till vårdinformationssystem för hälso- och sjukvårdspersonal*[8]. Dokumentet är fastställt av landstingsstyrelsen 2007 och är inte reviderat sedan Patientdatalagens och föreskrift 2008:14 ikraftträdande. Det aktuella dokumentet innehåller bl.a. referenser till lagstiftning som upphörde i samband med Patientdatalagen.

Behörighetshantering är också omnämnt i dokument *Övergripande regelverk vid logguppföljning*[9]. I detta dokument hänvisas till att landstinget skall bestämma villkor för tilldelning av behörighet för åtkomst till patientuppgifter och att verksamhetschefen, med utgångspunkt från vad landstinget bestämt, skall ansvara för att utdelade behörigheter för åtkomst till patientuppgifter är ändamålsenliga och förenliga med användarnas aktuella arbetsuppgifter. Dessutom ansvarar verksamhetschefen för att användarna är informerade om de bestämmelser som gäller för hantering av patientuppgifter.

Enligt informationssäkerhetsansvarig är det respektive systemägare som är ansvarig för att utarbeta anvisningar för behörighetstilldelning för respektive vårdinformationssystem. Det finns ingen förteckning över vilka vårdsystem där en behovs- och riskanalys har genomförts inför tilldelning av behörigheter.

Vad gäller journalsystemet COSMIC, som är ett av landstingets mest centrala vårdsystem, har ingen behovs- och riskanalys genomförts på de behörigheter som tilldelas användarna.

Tilldelning av behörigheter i COSMIC sker automatiskt när en anställd läggs upp i LiV-katalogen[10]. Ansvaret för att hålla LiV-katalogen uppdaterad ligger i linjen hos respektive chef. Tilldelning av behörigheter i COSMIC följer den i LiV-katalogen angivna yrkestillhörigheten samt verksamhetstillhörigheten. Det finns också ett antal specialbehörigheter på individ- respektive gruppnivå som kan tilldelas av respektive verksamhets systemadministratör.

Då behörighetstilldelningen till COSMIC sker automatiskt utifrån den i livkatalogen angivna yrkestillhörigheten framgår det inte hur verksamhetschefen tillämpar det som är angivet i dokument *Övergripande regelverk vid logguppföljning*, se ovan. Representant för ett av verksamhetsområdena uppger att det inte finns någon rutin på verksamhetsnivå för hur individuell tilldelning av behörigheter ska gå till. Det har inte heller genomförts någon behovs- och riskanalys på de behörigheter som används på verksamhetsnivå.

En annan verksamhetsföreträdare konstaterar att rutinen är att individuell tilldelning av behörigheter i normalfallet följer yrkestillhörighet. Därutöver tilldelas ibland särskilda behörigheter då en verksamhetschef individuellt tilldelat viss

[8] LK/071193, fastställda av landstingsstyrelsen 2007-10-16
[9] LK/090894, daterat 090529. Beslutat i dåvarande stabschefgrupp.
[10] Landstinget I Värmlands interna förteckning över sina anställda

personal arbetsuppgifter som kräver en särskild behörighet. Dessa särskilda behörigheter följs av en skriftlig delegation.

Vad gäller vissa delar av COSMIC är åtkomsten generellt begränsad. Det gäller journalanteckningar inom psykiatriska kliniken, kurators journalanteckningar på kvinnokliniken, journalanteckningar inom infektionskliniken för vissa patientgrupper samt vissa laboratoriesvar. Det framgår inte om det gjorts någon behovs- och riskanalys till grund för den begränsade åtkomsten till dessa delar av journalen. I övrigt finns inga begränsningar i vilken information som är möjlig att få åtkomst till.

Enligt föreskriften ska vårdgivaren ansvara för att information om vilka vårdenheter som har uppgifter om en viss patient inte kan göras tillgänglig utan att den behörige användaren gör ett aktivt val, dvs. gör ett ställningstagande till, om han eller hon har rätt att ta del av dessa uppgifter. Patientuppgifterna hos dessa vårdenheter får sedan inte göras tillgängliga utan att den behörige användaren gör ytterligare ett aktivt val. Det finns i dagsläget inget stöd i COSMIC för detta. Enligt systemansvarig är denna funktionalitet planerad att implementeras i augusti 2012.

Enligt Patientdatalagen måste det finnas möjlighet att spärra uppgifter i samtliga IT-system som innehåller vårddokumentation. Denna funktionalitet finns inte för COSMIC i dagsläget utan är planerad att implementeras i augusti 2012.

Vad gäller säkerhetskopiering anges i föreskrift 2008:14: *Vårdgivaren ska ansvara för att det i ledningssystemet finns rutiner för säkerhetskopiering av patientuppgifter. Av rutinerna ska det framgå med vilken periodicitet säkerhetskopieringen ska göras, hur länge säkerhetskopiorna ska sparas, och hur ofta återläsningstester ska göras*. I dokument ”Riktlinjer och regler för IT-säkerhet”[11] anges att ”intervallen för säkerhetskopieringen bestäms utifrån systemägarens krav på informationens aktualitet vid återstart från en säkerhetskopia. Det är systemägaren som tillsammans med driftsansvariga fastställer i driftsinstruktionen dessa regler”.

### 3.4.2 Bedömning

- Vi bedömer att landstingsstyrelsen inte lever upp till PDL och föreskriftens 2008:14 krav på behörighetstilldelning för samtliga vårdinformationssystem.

- Vi bedömer att det är en brist att det inte är gjort någon behovs- och riskanalys på de behörigheter som används i COSMIC, ett av landstingets mest centrala vårdsystem.

- Vår bedömning är att landstingsstyrelsen inte säkerställt lagens och föreskriftens krav på spärrhantering.

[11] Utfärdat 2010-01-13, senast reviderat 2011-08-15

**Förslag till åtgärder:**

- Säkerställ att det görs en behovs- och riskanalys inför tilldelning och kontinuerlig uppföljning av behörigheter på samtliga vårdsystem.

- Revidera omgående dokument *Riktlinje för tillgång till vårdinformationssystem för hälso- och sjukvårdspersonal* så att den följer och refererar till Patientdatalagen och föreskrift 2008:14. Skapa en rutin för att kontinuerlig följa upp och revidera detta dokument.

- Se över beskrivningen av behörighetstilldelning i dokument *Övergripande regelverk vid logguppföljning* och jämför den med den praktiska tillämpningen som utgår från yrkestillhörighet i LiV-katalogen. Säkerställ följsamhet till lag och föreskrift i tillämpningen.

## 3.5 Kontroll av åtkomst – spårbarhet

*Inom detta område är kontrollen av åtkomst till logginformation central, liksom spårbarheten i denna information.*

### 3.5.1 Iakttagelser

Vad gäller åtkomstkontroll ska vårdgivaren enligt 4 kap. 3 § patientdatalagen göra systematiska och återkommande kontroller på om någon obehörig kommer åt patientuppgifter. Detta kompletteras sedan av 2 kap. 11 § SOSFS 2008:14, där det bl.a. framgår att vårdgivaren ska ansvara för att det finns rutiner som säkerställer att:

1. det av dokumentationen av åtkomsten (loggarna) framgår vilka åtgärder som har vidtagits med patientuppgifterna,

2. det av loggarna framgår vid vilken vårdenhet och vid vilken tidpunkt åtgärderna har vidtagits,

3. användarens och patientens identitet framgår av loggarna, och

4. systematiska och återkommande stickprovskontroller av loggarna görs.

Regelverk för logguppföljning skall finnas för varje journalsystem inom landstinget enligt dokument Övergripande regelverk vid logguppföljning. Enligt uppgift finns det idag för journalsystemen Cosmic, Profdoc och Swedestar. Det framgår inte vad som gäller för övriga vårdinformationssystem annat än journalsystemen. Det framgår inte heller om alla vårdinformationssystem har stöd för logghantering.

Vad gäller journalsystemet COSMIC finns övergripande dokument *Riktlinjer för logghantering i COSMIC*[12]. Dokumentet är från 2006 och det framgår inte när det är reviderat. Regelverket beskriver ansvar, befogenheter, genomförande mm. av

[12] Daterat 2006-09-18, LK/050301

logguppföljning och logganalys. Av de intervjuade verksamhetsföreträdarna har lämnats lokala rutiner som beskriver hanteringen för det aktuella verksamhetsområdet.

Regelverket beskriver även tillvägagångssättet när en patient begär information om vilka som har tagit del av uppgifterna om patienten. Riktlinjen anger att innehållet i loggen till patienten skall vara begriplig och innehålla information om vem (inkl. befattning och vårdenhet) som har haft tillgång till journaltexten samt vid vilken tidpunkt.

### 3.5.2 Bedömning

- Övergripande regelverk vid logguppföljning är framtaget vilket vi finner tillfredsställande. Däremot framgår det inte i regelverket vad som gäller för logguppföljning för övriga vårdinformationssystem annat än journalsystem.

**Förslag till åtgärder:**

- Vidga *Övergripande regelverk vid logguppföljning* till att omfatta samtliga vårdinformationssystem. Utforma rutiner för uppföljning för att säkerställa regelverkets efterlevnad.

- Revidera dokument *Riktlinjer för logghantering i COSMIC*. Utforma rutiner för uppföljning för att säkerställa riktlinjernas efterlevnad.

## 3.6 Rutiner för journalföring

*Inom detta område granskas rutiner för journalföring och hantering av åtkomst till patientuppgifter, samt inhämtande av godkännande av patient vid sammanhållen journalföring.*

### 3.6.1 Iakttagelser

I föreskriftens 2 kap 2 § anges att informationssäkerhetspolicyn ska säkerställa att patientuppgifter i vårdgivarens dokumentation är åtkomliga och användbara för den som är behörig. Flera av de intervjuade redovisar en brist i åtkomlighet då det finns långa ledtider mellan diktat av journalanteckning och dokumentation av dessa. Ledtiderna utgör en stor patientsäkerhetsrisk då nödvändig information inte är åtkomlig vid patientkontakt. Här pekar intervjupersonerna också på vikten att informationssäkerhetsarbetet måste vara en integrerad del av patientsäkerhetsarbetet.

Vad gäller själva dokumentationen i COSMIC har mallar tagits fram per verksamhetsområde. Även begrepp och regelverk för sökord togs fram i införandefasen. För att säkerställa att viss information alltid loggas i journalen är vissa delar obligatoriska att fylla i. Det pågår en översyn av mallarna idag då det enligt systemansvarig finns för många mallar. Ambitionen är att översynen ska leda till att mallarna följer Socialstyrelsens standard.

Landstingsarkivarie tillika personuppgiftsombud har i ett PM[13], ”Sökning efter patientjournaler”, aktualiserat frågan om sökning efter patientjournaler. Denna fråga har bl.a. bäring på föreskriftens formulering om *hantering av åtkomst till patientuppgifter*. Frågeställningen gäller på vilket sätt och i vilken omfattning ska sökning gå till på Landstingsarkivet och hos landstingsarkivarien tillika personuppgiftsombudet efter patientjournaler. I det aktuella PM’et beskrivs att landstingets patientjournalbestånd och personuppgiftsbehandlingar rymmer ett stort spektra av olika media (papper, mikrofilmade dokument, inskannade dokument osv.). Det finns inget heltäckande register som visar var patientjournaler finns och därmed kan inte dagens hanterande av patientjournaler utifrån perspektivet sökning sägas vara patientsäkert.

### *3.6.2 Bedömning*

- Vi bedömer inte rutinen för journalföring och hantering av åtkomst till patientuppgifter är tillfredsställande i de delar som avser att dokumentation ska vara åtkomlig och användbar utan fördröjning för den som är behörig.

**Förslag till åtgärder:**

- Utred snarast orsakerna till varför det finns brister i åtkomst till patientinformation samt hur dessa ska åtgärdas.

- Säkerställ att arbetet med översyn av mallar i COSMIC enligt Socialstyrelsens standard färdigställs och därefter kontinuerligt revideras.

- Se över och ta ställning till de förslag till åtgärder som lämnas i PM ”Sökning efter patientjournaler” för att på så sätt identifiera ambitionsnivån för sökandet efter patientjournaler.

## *3.7 Incidenthantering*

*Inom detta område granskas hantering och uppföljning av incidenter.*

### *3.7.1 Iakttagelser*

I landstinget finns, sedan 2009, ett elektroniskt system för avvikelsehantering. Systemet underlättar ett systematiskt arbetssätt för avvikelsehantering. Riktlinjer och råd för avvikelsehantering har tagits fram även om fortsatt arbete krävs för att uppnå följsamhet. Ett av de mest frekventa avvikelseområdena är vårddokumentation och informationsöverföring[14]. Det går i dagsläget inte att närmare klassificera avvikelser för att tydligt identifiera dessa relaterat till Patientdatalagen och/eller till föreskrift 2008:14. Verksamhetsföreträdarna uppger att de använder systemet för registrering av ärenden som avser brister i informationssäkerheten.

[13] Daterat 2011-11-07, LK/111872
[14] Från Patientsäkerhetsberättelse 2010

I uppdraget för ”Klinisk Beslutsgrupp för Vårdsystem” anges att hantera avvikelser rörande vårdsystem som rör systemövergripande aspekter eller driftstörningar, säkerhet mm. Sedan KBV skapades i januari 2011 har det inte förekommit några stora störningar. I det fall en systemövergripande avvikelse registreras, kommer KBV att delta i vidare händelseanalys och behandla de eventuella åtgärder som kommer fram av den.

### 3.7.2 Bedömning

- Landstinget har ett avvikelsehanteringssystem vilket vi finner tillfredsställande. Däremot går det inte att få ut statistik som visar på avvikelser där brister i informationssäkerhet är identifierade.

**Förslag till åtgärder:**

- Säkerställ att avvikelser klassificeras på ett sätt som möjliggör utdata där ärenden som avser brister i informationssäkerheten relaterat lag och föreskrift går att identifiera.

- Identifiera vilka funktioner som är berörda av dessa avvikelser och säkerställ att dessa involveras i analys och åtgärder.

## 3.8 Förankring i organisationen

*Inom detta område granskas arbetet med förankring i organisationen, detta innefattar bl.a. informations- och utbildningsinsatser.*

### 3.8.1 Iakttagelser

Flertalet läkarsekreterare har, inom ramen för särskilt EU-projekt, fått utbildning i Patientdatalagen. I övrigt har inga systematiska utbildnings- eller informationsinsatser ägt rum. I de fall enskilda verksamheter vänt sig till landstingets jurist med frågeställningar relaterade till lagen har juristen bistått med denna information. En verksamhetsföreträdare anger att patientsäkerhet, sekretess och lagstiftning diskuteras utifrån aktuella frågeställningar och exempel så gott som varje vecka på arbetsplatsträffarna.

De intervjuade verksamhetsföreträdarna efterfrågar utbildning och information kring Patientdatalagen och föreskriften. De jämför med den omfattande information som getts i samband med Patientsäkerhetslagens införande 1/1 2011.

Sedan cirka ett år tillbaka ges en generell utbildning för alla verksamhetschefer i landstinget. Denna utbildning omfattar vissa delområden inom gällande lagar och föreskrifter såsom medicinsk teknik och informationssäkerhet.

### 3.8.2 Bedömning

- Den riktade utbildningsinsatsen för läkarsekreterare samt den generella utbildning som samtliga verksamhetschefer genomgår finner vi tillfredsställande. Däremot saknas riktade utbildningsinsatser för Patientdatalagen och föreskrift 2008:14 som omfattar samtlig personal.

**Förslag till åtgärder**:

- Följ upp och säkerställ att den information som givits verksamhetscheferna kommer övrig personal till del på ett strukturerat sätt.

- Genomför en riktad informationsinsats till samtlig personal, även de inom administrativa enheter, rörande Patientdatalagen och föreskrift 2008:14. Komplettera med informationsmaterial.

# 4 Sammanställning av förslag till åtgärder inklusive prioritering

| Prioritering av åtgärder – **prioritet HÖG** |
|---|
| ➢ Ge direktiv om ta fram en informationssäkerhetspolicy och prioritera arbetet med att ta fram en sådan. Skapa en rutin för att kontinuerlig följa upp och revidera denna policy. |
| ➢ Tydliggör roller, ansvar, avgränsningar mellan de olika funktioner och grupperingar som arbetar med frågor som relaterar till PDL och föreskriften. Beskriv och kommunicera mandat, syfte och sammanhang för samtliga funktioner och grupperingar. Säkerställ att grupperna företräds av funktioner som bidrar till gruppens förväntade effekt. |
| ➢ Upprätta en samlad förteckning av vilka vårdinformationssystem som innehåller patientuppgifter och i vilken utsträckning de möter kraven i Patientdatalagen och föreskrift 2008:14 |
| ➢ Utred snarast orsakerna till varför det finns brister i åtkomst till patientinformation samt hur dessa ska åtgärdas. |
| ➢ Genomför en riktad informationsinsats till samtlig personal, även de inom administrativa enheter, rörande Patientdatalagen och föreskrift 2008:14. Komplettera med informationsmaterial. |

| Prioritering av åtgärder – **prioritet MEDEL** |
|---|
| ➢ Säkerställ att informationssäkerhetsansvarigs organisatoriska tillhörighet till Landstings-IT *inte* innebär att ansvaret att styra och ställa krav på informationssäkerheten läggs på IT-avdelningen. |
| ➢ Ta fram skriftlig dokumentation som tydligt beskriver vilket ansvar vårdgivaren har lagt på verksamhetschefen. |
| ➢ Säkerställ att verksamhetscheferna tar fram, fastställer och dokumenterar ändamålsenliga rutiner för informationshanteringen. |
| ➢ Revidera *Informationshandboken*. Säkerställ att *Informationshandboken* beaktar Personuppgiftslagen. Skapa en rutin för att kontinuerlig följa upp och revidera denna handbok. |
| ➢ Säkerställ att det görs en behovs- och riskanalys inför tilldelning och kontinuerlig uppföljning av behörigheter på samtliga vårdsystem. |
| ➢ Se över beskrivningen av behörighetstilldelning i dokument *Övergripande regelverk vid logguppföljning* och jämför den med den praktiska tillämpningen som utgår från yrkestillhörighet i LiV-katalogen. Säkerställ följsamhet till lag och föreskrift i tillämpningen. |
| ➢ Vidga *Övergripande regelverk vid logguppföljning* till att omfatta samtliga vårdinformationssystem. Utforma rutiner för uppföljning för att säkerställa regelverkets efterlevnad. |
| ➢ Revidera dokument *Riktlinjer för logghantering i COSMIC*. Utforma rutiner för uppföljning för att säkerställa riktlinjernas efterlevnad. |
| ➢ Säkerställ att avvikelser klassificeras på ett sätt som möjliggör utdata där ärenden som avser brister i informationssäkerheten relaterat lag och föreskrift går att identifiera. |
| ➢ Identifiera vilka funktioner som är berörda av dessa avvikelser och säkerställ att dessa involveras i analys och åtgärder. |
| ➢ Följ upp och säkerställ att den information som givits verksamhetscheferna kommer övrig personal till del på ett strukturerat sätt. |

| Prioritering av åtgärder – **prioritet LÅG** |
| --- |
| ➢ Revidera omgående dokument *Riktlinje för tillgång till vårdinformationssystem för hälso- och sjukvårdspersonal* så att den följer och refererar till Patientdatalagen och föreskrift 2008:14. Skapa en rutin för att kontinuerlig följa upp och revidera detta dokument. |
| ➢ Säkerställ att arbetet med översyn av mallar i COSMIC enligt Socialstyrelsens standard färdigställs och därefter kontinuerligt revideras. |

2012-0x-xx

*Eva Lidmark, projektledare*

*Jon Arwidson, uppdragsledare*