Revisionsrapport -

Granskning av informationssäkerhet – patientinformation

Landstinget i Värmland

Eva Lidmark
Peter Aschberg

18 november 2014

pwc

Innehållsförteckning

1 Sammanfattning

PwC har av revisorerna i Landstinget i Värmland fått i uppdrag att genomföra en granskning av informationssäkerhet avseende patientinformation. Syftet med den aktuella granskningen är att ta fram underlag för att bedöma om landstingsstyrelsen säkerställt en ändamålsenlig informationssäkerhet rörande patientinformation samt hur landstingstyrelsen hanterat de frågeställningar som togs upp i revisorernas rapport nr 5 -11, *Granskning av efterlevnad av patientdatalagen (2008:355)*.

Revisionsfrågor och granskningsresultat:

- *Har landstingsstyrelsen sett till att genomföra de förbättringsåtgärder som föreslås i granskningsrapporten?*
  De förbättringsåtgärder som föreslogs i revisorernas rapport nr 5 -11 har till vissa delar genomförts varav den viktigaste är framtagande av Informationssäkerhetspolicy och Riktlinje för informationssäkerhet. Granskningen visar att det finns ytterligare åtgärder som behöver vidtas.

- *Har landstingstyrelsen fått en kontinuerlig återrapportering av genomförda åtgärder i enlighet med landstingstyrelsens svar till revisorerna?*
  Landstingstyrelsen har vid ett tillfälle fått återrapportering av genomförda åtgärder. Ytterligare avrapportering borde ha skett för att säkerställa att planerade åtgärder blev vidtagna. Oberoende av denna återrapportering får landstingstyrelsen årligen en informationssäkerhetsrapport som följer kraven på innehåll enligt Socialstyrelsens föreskrift. Granskningen visar att denna återrapportering kan förbättras sett till frekvens och utvidgning av innehåll.

- *Har landstingsstyrelsen genom styrning, uppföljning och intern kontroll säkerställt att landstinget nu efterlever gällande bestämmelser?*
  Genom upprättande av informationssäkerhetspolicy och riktlinjer för informationssäkerhet har landstingstyrelsen förbättrat förutsättningarna för styrning, uppföljning och intern kontroll och efterlever i större utsträckning än vid förra granskningstillfället (2011) gällande bestämmelser. Granskningen visar att det finns delar av informationssäkerhetsarbetet som kan förbättras avseende styrning, uppföljning och intern kontroll. Frånvaron av en fastställd handlingsplan för informationssäkerhetsarbetet är ett avsteg från den av landstingsfullmäktige antagna informationssäkerhetspolicyn.

- *Efterlever Landstinget i Värmland nu patientdatalagen med tillhörande föreskrifter?*

Landstinget i Värmland efterlever till större delar än vid förra granskningstillfället patientdatalagen med tillhörande föreskrifter. Granskningen visar att det finns förbättringar att göra för att ytterligare säkerställa efterlevnaden.

- *Om det kvarstår brister, vilka förbättringsåtgärder behöver vidtas?*
  Det kvarstår ett antal brister och en samlad förteckning över förslag till förbättringar redovisas i bilaga 1.

Vår samlade bedömning är att landstingsstyrelsen sedan föregående granskning, bland annat genom framtagande av informationssäkerhetspolicy, riktlinjer för informationssäkerhet samt andra styrande dokument, har förbättrat förutsättningarna för styrning, uppföljning och intern kontroll gällande informationssäkerhetsarbetet och därmed också för efterlevnad av gällande regelverk. Vi bedömer dock att det kvarstår ett antal brister och att ett fortsatt arbete måste ske, där några av de viktigaste områdena är att tillse att det fastställs en handlingsplan för informationssäkerhetsarbetet samt att det tillskapas organisatoriska förutsättningar för att patientsäkerhetsarbetet och informationssäkerhetsarbetet kan bedrivas på ett integrerat och effektivt sätt.

2 Inledning

2.1 Revisionskriterier

Granskningen tar sin utgångspunkt i Patientdatalagen (2008:355) samt Socialstyrelsens 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. Förarbete till lagen framgår av prop. 2007/08:126. I sekretesslagen (1980:100) infördes 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. La-

[1] understödjande

gen ska även främja kostnadseffektivitet, att personuppgifter utformas och i övrigt behandlas så att patienters och övriga registrerades integritet respekteras.

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.

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 §).

2.2 Uppdrag, revisionsfrågor och metod

PwC har av revisorerna i Landstinget i Värmland fått i uppdrag att genomföra en granskning av informationssäkerhet avseende patientinformation. Syftet med den aktuella granskningen är att ta fram underlag för att bedöma om landstingsstyrelsen nu säkerställt en ändamålsenlig informationssäkerhet rörande patientinformation samt hur landstingstyrelsen hanterat de frågeställningar som togs upp i revisorernas rapport nr 5 -11, *Granskning av efterlevnad av patientdatalagen (2008:355)*. I bilaga 2 redovisas vilka åtgärder som är vidtagna sedan rapport nr 5-11.

De revisionsfrågor som revisorerna önskar få besvarade är:

- Har landstingsstyrelsen sett till att genomföra de förbättringsåtgärder som föreslås i granskningsrapporten?
- Har landstingstyrelsen fått en kontinuerlig återrapportering av genomförda åtgärder i enlighet med landstingstyrelsens svar till revisorerna?
- Har landstingsstyrelsen genom styrning, uppföljning och intern kontroll säkerställt att landstinget nu efterlever gällande bestämmelser?
- Efterlever Landstinget i Värmland nu patientdatalagen med tillhörande föreskrifter?
- Om det kvarstår brister, vilka förbättringsåtgärder behöver vidtas?

Granskningen har genomförts genom intervjuer och genom granskning av dokumentation. Intervjupersoner framgår i bilaga 1. Rapporten har sakgranskats av intervjupersonerna.

3 Granskningsresultat

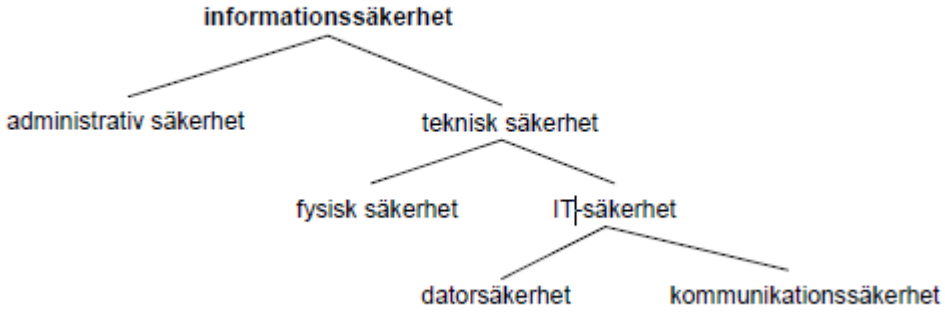
3.1 Informations-/IT-säkerhetspolicy

Inom detta område redovisas de styrande dokumenten, såväl utformning som innehåll och tillämpning.

3.1.1 Iakttagelser

Enligt föreskriften 2008:14 ska vårdgivaren ge direktiv och säkerställa att det i verksamhetens ledningssystem för kvalitet och patientsäkerhet finns en dokumenterad informationssäkerhetspolicy. Landstingsfullmäktige har antagit en *informationssäkerhetspolicy*[2]. I den framgår att målet för landstingets informationssäkerhetsarbete är att skydda informationen inom verksamheten. Skyddet ska vara anpassat till skyddsvärde, risk och lagkrav och därigenom möjliggöra för landstingets verksamheter att uppnå sina mål.

Till informationssäkerhetspolicyn finns även fastställda *Riktlinjer för informationssäkerhet*[3]. Riktlinjerna är en konkretisering av landstingets informationssäkerhetspolicy och är styrande för landstingets informationshantering. I riktlinjerna åskådliggörs de olika delarna inom informationssäkerhet i följande modell:



Administrativ säkerhet innefattar skyddsåtgärder av administrativ art. Exempel på det är hur styrning och uppföljning av informationssäkerheten ska ske, hur ansvar

[2] Informationssäkerhetspolicy, fastställd av landstingsfullmäktige, 2012-11-28, LK/121686
[3] Riktlinjer för informationssäkerhet, fastställd av landstingsdirektör, 2012-11-28, LK/121686

för informationssäkerheten ska fördelas, hur åtkomst till informationen ska regleras och hur rutinerna ska utformas. Information och utbildning är också en viktig del. Riktlinjer för informationssäkerhet är en del av den administrativa säkerheten. I riktlinjen anges att informationssäkerhetsarbetet berör hela landstingets verksamhet. Det framgår att det är positivt att policy och riktlinjer finns framtagna.

Ytterligare ett styrande dokument med bäring på informationssäkerhetsarbetet är framtaget. Det är ett vårdgivardirektiv[4] för *Informationshantering och journalföring i hälso- och sjukvården*[5]. Styrande och stödjande dokument relaterade till informationssäkerhetsarbetet är integrerade i ledningssystemet. Det är känt var informationen finns att tillgå.

I landstinget ges regelbundet en introduktionsutbildning för nya verksamhetschefer. En del i denna utbildning avser informationssäkerhet och ges av informationssäkerhetsansvarig. Verksamhetschef ansvarar, enligt vårddirektivet, för implementering och följsamhet till riktlinjerna. I samband med implementering av riktlinjerna ska behövliga utbildningsinsatser göras. Personalen anses ha god kännedom om och tillämpar policy, riktlinjer och övriga regelverk men det är en ständig utmaning att hålla kunskaperna uppdaterade.

Det finns ytterligare dokument framtagna för att underlätta och stärka informationssäkerhetsarbetet. Dessa är till exempel *Informationshantering och journalföring i hälso- och sjukvården*[6], *Rutiner vid begäran om journalkopior och utdrag av personuppgiftsbehandlingar*[7], *Riktlinjer för hantering av skyddade personuppgifter inom hälso- och sjukvården samt tandvården*[8], *Rutin för remisshantering – god klinisk praxis*[9] samt *Utlämnande av journalhandlingar*[10].

Förutom dessa exempel på landstingsövergripande dokument lämnas också exempel på lokala rutiner.

Vad gäller uppföljning av policyn anges att landstingets informationssäkerhetsarbete ska rapporteras till landstingsstyrelsen minst en gång per år. Detta görs genom den årliga informationssäkerhetsrapporten som behandlas av landstingsstyrelsen. Rapportens innehåll följer det som anges i föreskrift 2008:14[11]. Återrapportering av de åtgärder som vidtogs med anledning av revisorernas rapport 05-11 skedde vid ett tillfälle, september 2012.

[4] Vårdgivardirektiv anger den politiska ledningens tolkning av hur landstinget ska uppfylla lagar och andra författningar.
[5] Fastställt av Landstingtingsstyrelsen, giltigt 2014-01-01–2016-12-31
[6] Vårdgivardirektiv, 2014-01-01—2016-12-31
[7] Rutin, giltighetstid 2011-12-01—2014-11-30
[8] Riktlinje, giltighetstid 2013-01-01—2015-12-31
[9] Rutin, giltighetstid 2013-12-01—2015-12-31
[10] Riktlinje, giltighetstid 2012-11-01—2015-10-31
[11] 2008:14, 2 kap, § 3

Vad gäller uppföljning av riktlinjerna anges att landstingsstyrelsen har det övergripande ansvaret för informationssäkerheten inom landstinget och därmed för samordning och uppföljning av informationssäkerheten. Den strategiska gruppen för informationssäkerhet (SGI) har till uppgift att främja, stödja, samordna och följa upp landstingets informationssäkerhetsarbete på en övergripande nivå. Sedan en tid har SGI inga möten. Det beror bland annat på att gruppen avvaktar resultatet av det pågående utredningsarbetet avseende framtida utformning och organisering för ny informationssäkerhetsansvarig.

I vårdgivardirektivet framgår att en skriftlig uppföljning av vårdgivardirektivet sker en gång per år i landstingsstyrelsen genom att divisionerna i den årliga patientsäkerhetsberättelsen redogör för hur man arbetat med samtliga vårdgivardirektiv, däribland det som behandlar informationshantering och journalföring

I landstinget pågår ett arbete med att ta fram en förteckning över vilka vårdinformationssystem som innehåller patientuppgifter. Enligt uppgift rör det sig om över 60 system men det exakta antalet är oklart. För den delmängd av system som ingår i objektfamiljen Patientjournal är alla system inventerade. För de system som saknar systemägare, och/eller har få användare och/eller inte möter kraven i patientdatalagen, är en process för systemavveckling framtagen.

3.1.2 Bedömning

- Det är tillfredsställande att det finns en informationssäkerhetspolicy samt riktlinjer för informationssäkerhet. Genom dessa dokument har en struktur skapats för styrningen av arbetet med informationssäkerhet. Vi bedömer att dokumenten till stora delar är ändamålsenliga.

- Det är tillfredsställande att det finns ytterligare rutiner, riktlinjer och vårdgivardirektiv som stödjer informationssäkerhetsarbetet.

- Det är tillfredsställande att den årliga informationssäkerhetsrapport till landstingsstyrelsen till sitt innehåll följer det som anges i föreskrift 2008:14 . Rapporten kan förbättras genom att även innehålla förslag på var ansvaret för de listade förbättringsområdena bör ligga.

- Vid avrapportering av vidtagna åtgärder efter revisorernas rapport 05-11 (september 2012) kvarstod ytterligare punkter att åtgärda. Ytterligare avrapportering borde ha skett för att säkerställa att planerade åtgärder blev vidtagna.

- För att ytterligare höja kvalitén på rapporten kan den även återrapportera på ytterligare delar i landstingets riktlinje för informationssäkerhet. Rapporteringsfrekvensen bör utökas till två gånger per år.

- Det finns oklarheter i den övergripande uppföljning som ska ske av efterlevnad av policy och riktlinjer. Detta då ansvaret för den övergripande uppföljningen ligger på en gruppering som inte är aktiv.

- Det är en brist att det inte finns en komplett förteckning över vilka vårdinformationssystem som innehåller patientuppgifter. Detta var en anmärkning även vid granskningen 2011.

- Arbetet med systemavveckling enligt den framtagna processen för systemavveckling bör prioriteras.

Förslag till åtgärder:

- Utveckla den årliga informationssäkerhetsrapporten till att återrapportera på fler delar än de som föreskriften påbjuder. T ex kan en utgångspunkt vara att återrapportera på ytterligare områden relaterat till landstingets riktlinjer. Rapporten kan också innehålla förslag på var ansvaret för de listade förbättringsområdena bör ligga. Överväg 2 rapporteringstillfällen per år.

- Tydliggör vem som ansvarar för den övergripande uppföljningen av efterlevnad av policy och riktlinjer då detta övergripande uppföljningsansvar ligger på en gruppering som inte är aktiv.

- Färdigställ förteckningen över vilka vårdinformationssystem som innehåller patientuppgifter samt prioritera arbetet med systemavveckling.

3.2 Landstingsstyrelsens övergripande säkerhetsstyrning

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

3.2.1 Iakttagelser

Informationssäkerhet är en patientsäkerhetsfråga under vårdgivarens ansvar. Informationssäkerheten ska ingå som en del av vårdgivarens ledningssystem för kvalitet och patientsäkerhet[12]. Ledningssystemet är ledningens verktyg för att tydliggöra hur organisationen styrs och leds. Arbetet med ledningssystemet är under uppbyggnad men är också ett ständigt pågående arbete enligt intervjupersonerna. Ledningssystemet, som benämns ”Vårt arbetssätt” på intranätet, spänner över gällande lagstiftning, landstingsplan inklusive mål, verksamhetsplaner samt över styrande dokument över definierade områden.

I landstinget finns en informationssäkerhetsansvarig. Det framgår att denna funktion är mycket viktig och bidrar på ett positivt sätt till informationssäkerhetsarbetet. Det framförs önskemål om att funktionens roll och mandat ska tydliggöras. I det att nuvarande informationssäkerhetsansvarig går i pension hösten 2014 har en över-

[12] SOSFS 2005:12

syn[13] gjorts av funktionens framtida utformning och organisering. Inga beslut är ännu tagna i denna fråga.

I riktlinjerna för informationssäkerhet beskrivs också organisation av informationssäkerheten. Mer om organisation, roller och ansvar redovisas under punkt 3.3.

Det finns brister i den övergripande styrningen av informationssäkerhetsarbetet. Bristerna yttrar sig bland annat i frånvaron av fungerande struktur för hur beslut i och direktiv från landstingsstyrelsen (LS) kommuniceras ut till underliggande ansvarsnivåer.

Ett praktiskt exempel på brister i den övergripande styrningen av informationssäkerhetsarbetet ges via arbetet med den årliga informationssäkerhetsrapporten. Informationssäkerhetsrapporten listar bland annat vilka förbättringsåtgärder som behöver vidtas. Landstingsstyrelsens behandling av rapporten resulterar inte i något beslut eller direktiv och därmed uppstår svårigheter att följa upp vem som fått ansvaret att vidta vilka åtgärder[14].

Den modell och organisation för förvaltningsstyrning som landstinget valt att tillämpa för sina förvaltningsobjekt fungerar inte optimalt vilket får negativa konsekvenser för informationssäkerhetsarbetet. I den valda modellen finns samtliga resurser organiserade inom IT-organisationen, även de som företräder verksamhetsperspektivet för de objekt som förvaltas. Undantaget finns för objektägarna på verksamhetssidan som organisatoriskt ligger utanför IT-organisationen.

3.2.2 Bedömning

- Det är tillfredsställande att ledningssystemet ”Vårt arbetssätt” är under aktiv uppbyggnad, att styrdokumenten för informationssäkerhetsarbetet är integrerade i ledningssystemet och att det är känt i verksamheten var dessa dokument finns att tillgå.

- Det är tillfredsställande att landstinget har en informationssäkerhetsansvarig.

- Det finns behov av förtydligande vad gäller informationssäkerhetsansvariges roll, mandat, besluts- och kommunikationsvägar.

- Det finns brister i den del av styrningen som avser hur beslut och direktiv från landstingsstyrelsen avseende informationssäkerhet kommuniceras till linjeorganisationen. Denna brist gör sig även gällande när det kommer till uppföljning av fattade beslut/givna direktiv inom detta område. Denna brist får direkt påverkan på uppföljningen av den årliga informationssäkerhetsrapporten och är därmed inte tillfredsställande ur ett internkontrollperspektiv.

[13] Informationssäkerhetsansvarig i LiV, underlag för framtida utformning och organisering. PM 2014-05-14
[14] Uppföljning av den årliga rapporten sker på LS sammanträde i september.

- Det sätt som landstinget valt att organisera sina resurser inom förvaltningsstyrning bör ses över för att säkerställa informationssäkerhetsperspektivet i den valda modellen.

Förslag till åtgärder:

- Skapa en större tydlighet i hanteringen av informationssäkerhetsärenden från LS så att det tydligt kommuniceras till linjen vilka beslut och direktiv som är tagna och förväntas åtgärdas av linjen samt vem som förväntas agera. Samma tydlighet behövs vad gäller uppföljning av åtgärder.

- Säkerställ att informationssäkerhetsansvariges roll och mandat tydliggörs i framtida utformning och organisering.

- Utvärdera tillämpningen av modellen för förvaltningsstyrning avseende informationssäkerhetsperspektivet.

3.3 Roller och ansvar

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

3.3.1 Iakttagelser

Genom informationspolicyn och riktlinjerna har en formell struktur skapats för arbetet med informationssäkerhet. I riktlinjerna tydliggörs roller och ansvar på följande sätt:

- *Landstingsfullmäktige* fastställer landstingets informationssäkerhetspolicy.

- *Landstingsstyrelsen* ansvarar för
  - att landstingets informationssäkerhetspolicy och riktlinjer för informationssäkerheten utarbetas och hålls aktuella,
  - samordningen av informationssäkerhetsarbetet i landstinget och ska därför *årligen* fastställa en handlingsplan för informationssäkerhetsarbetet,
  - att det utses en person som ansvarar för landstingets informationssäkerhetsarbete.

- *Landstingsdirektören* har landstingsstyrelsens uppdrag att tillse att informationssäkerhetsarbetet bedrivs så effektivt som möjligt genom att visa ett tydligt stöd och fördela resurser så att informationssäkerhetsmålet kan uppnås.

- *Informationssäkerhetsansvarig* verkställer samordningen av informationssäkerhetsarbetet inom landstinget och förvaltar landstingets informationssäkerhetspolicy, riktlinjer samt en övergripande handlingsplan för informationssäkerhet.

Vad gäller den övergripande handlingsplanen är den inte är framtagen. Vad gäller informationssäkerhetsansvarige uppfattas att rollen har oklara mandat och rapporteringsvägar samt att rollen varken finns i linjeorganisationen eller är en uttalad expertroll. Denna otydlighet innebär en svag tillgång till de ledningsfunktioner som har ansvaret för att ta fram den handlingsplan som sedan informationssäkerhetsansvarig ansvarar för att förvalta.

- Ansvaret för informationssäkerheten är kopplat till det delegerade verksamhetsansvaret. Det betyder att varje person som är ansvarig för en verksamhet också är ansvarig för informationssäkerheten i denna verksamhet. *Verksamhetschefen* har, inom sin verksamhet, ansvaret för att utforma och kommunicera anvisningar. I ansvaret ingår även att säkerställa att all informationshantering sker i enlighet med informationssäkerhetspolicy, riktlinjer och anvisningar samt att vid behov fastställa lokala instruktioner. Verksamhetschefens uppdrag och ansvar framgår i dokument ”*Uppdrag och ansvar för verksamhetschef*[15]”.

Det är generellt en utmaning att säkerställa att all personal har tagit del av övergripande och lokala riktlinjer och anvisningar. Detta på grund av att tillgänglig arbetstid inte räcker till för de informationsmängder som ska delges personalen. Inom division allmänmedicin har införandet av journalsystemet COSMIC gett ett gynnsamt läge att, integrerat med utbildning i systemet, utbilda i informationssäkerhet med tillhörande lagstiftning.

- *Informationsanvändare* är samtliga personer som i sin yrkesutövning hanterar information inom landstinget vilket inkluderar såväl anställda som andra användare. Informationsanvändarnas medverkan är väsentlig för en effektiv informationssäkerhet. De ska göras medvetna om sin skyldighet att ta del av och följa uppställda informationssäkerhetsregler liksom att rapportera informationssäkerhetsincidenter, funktionsfel och brister enligt fastställa rutiner.

- *Personuppgiftsombud* har bland annat till uppgift att tillse att personuppgifter behandlas på ett lagligt och korrekt sätt.

Rollen som personuppgiftsombud och vad den ska bidra med i informationssäkerhetsarbetet behöver tydliggöras ytterligare utöver vad som framgår i riktlinjen.

[15] LK/130637

- För att samordning och uppföljning av informationssäkerhetsarbetet ska kunna bedrivas effektivt ska det finnas en *strategisk grupp för informationssäkerhet (SGI*). Utöver informationssäkerhetansvarig ska gruppen bestå av IT-säkerhetsansvarig, arkivarie, jurist samt representanter från respektive division.

Sedan en tid har SGI inga möten. Det beror bland annat på att gruppen avvaktar resultatet av det pågående utredningsarbetet avseende framtida utformning och organisering för ny informationssäkerhetsansvarig. Det framkommer önskemål om att SIG's uppdrag, mandat och förväntad effekt tydliggörs samt till vem gruppens arbete ska avrapporteras.

Det finns önskemål om att det, i samband med den framtida utformningen och organiseringen för informationssäkerhetsansvarig, uttalas på vilket sätt chefläkarfunktionen ges en roll i informationssäkerhetsarbetet och på vilket sätt andra centrala grupperingar, som t ex grupperingen Klinisk Beslutsgrupp Vårdsystem (KBV), ska ges en roll. KBV är ett exempel på ytterligare en gruppering som arbetar med frågor relaterade till informationssäkerhetsarbetet utan att ha en definierad roll eller formellt ansvar enligt riktlinjerna för informationssäkerhet.

KBV arbetar utifrån ett direktiv[16] som i sju punkter anger gruppens uppdrag. Bland annat ska KBV ansvara för operativa beslut rörande LiV:s samtliga vårdsystem som ligger utanför direkt IT-förvaltning och i de fall uttalad systemförvaltningsgrupp och/eller objektägare inte hanterar sådana frågor. Informationssäkerhetssamordnaren ingår inte i KBV.

Inte heller har chefläkaren, vars uppdrag bland annat är att arbeta strategiskt med patientsäkerhet, någon roll i informationssäkerhetsarbetet enligt riktlinjerna. Det efterfrågas en bättre integration av patientsäkerhetsarbetet och informationssäkerhetsarbetet och att chefläkarens roll i informationssäkerhetsarbetet ska formaliseras.

3.3.2 Bedömning

- En handlingsplan för informationssäkerhetsarbetet finns inte framtagen vilket är ett avsteg från den av landstingsfullmäktige antagna policyn. Enligt policyn ska en sådan fastställas av landstingsstyrelsen.

- Informationsansvariges mandat och rapporteringsvägar behöver förtydligas. Informationssäkerhetsansvarig bör vara representerad i Klinisk Beslutsgrupp Vårdsystem.

- Ett stort antal roller och ansvar är beskrivna i riktlinjerna för informationssäkerhet vilket bedöms som positivt. För att åstadkomma större samordning av informationssäkerhetsarbetet finns det behov av att se över vilka ytterligare

[16] Klinisk Beslutsgrupp Vårdssystem – Organisation och Direktiv 2013-12-01—2016-12-13

grupperingar, funktioner och roller som på ett avgörande sätt är viktiga för informationssäkerhetsarbetet. Detta gäller t ex chefläkare tillika patientsäkerhetsansvarig och Klinisk Beslutsgrupp Vårdssystem.

- Det är tillfredsställande att det finns beskrivningar på verksamhetschefernas uppdrag och ansvar.

Förslag till åtgärder:

- Ta fram en handlingsplan för informationssäkerhetsarbetet enligt landstingsfullmäktiges antagna informationssäkerhetspolicy.

- Tydliggör informationsansvariges mandat och rapporteringsvägar samt överväg informationsansvariges deltagande i KBV.

- Gör en översyn över vilka ytterligare grupperingar, funktioner och roller som på ett avgörande sätt är viktiga för att uppnå större samordning av informationssäkerhetsarbetet. Komplettera sedan riktlinjerna med dessa grupperingars, funktioners och rollers ansvar.

3.4 Behörigheter och åtkomst

Inom detta område redovisas rutiner för behörigheter och åtkomst, såväl processer som vissa system granskas. Tekniska granskningar av behörighetsstruktur har inte gjorts. Delområden som omfattas är signering, spärrning och säkerhetskopiering av patientuppgifter.

3.4.1 Iakttagelser

Vad gäller behörighetstilldelning anges i 4 kap. 2 § PDL 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 bland annat 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.

I riktlinjerna för informationssäkerhet finns ett avsnitt som behandlar åtkomst till information. Där framgår det att all tillgång till elektronisk information inom landstinget ska styras med hjälp av följande administrativa och tekniska skyddsåtgärder: åtkomstadministration, åtkomstkontroll samt loggning och uppföljning.

Vad gäller åtkomstadministration bygger åtkomsträttigheten på användarens behörighet, arbetsuppgifter och organisatoriska tillhörighet. Som exempel ges att tilldelning av behörigheter i COSMIC sker utifrån den anställdes roll och enhet. I rutinen

Behörighetstilldelning, tillgång till vårddata i COSMIC[17], anges principerna för de olika behörighetstyperna i COSMIC. I dokument *Behörighetsprofiler COSMIC*[18] åskådliggörs, via en rollmatris, de aktuella behörighetsprofilerna och vilken typ av rättigheter som respektive profil har i systemets olika moduler.

Med anledning av en tillsyn som gjordes 2013[19] av Datainspektionen[20] (DI) redovisade landstinget hur vårdgivaransvaret att genomföra en behovs- och riskanalys inom ramen för behörighetstilldelning/-styrning uppfylls för huvudjournalsystemet COSMIC. Landstinget angav i sitt svar till DI att behörighetsstyrningen i COSMIC inte är individbaserad utan utgår från roll och enhet. DI har inte återkommit med invändningar efter den redovisningen. I svaret till DI angavs även att en riktlinje för behovs- och riskanalys vid tilldelning av rättigheter som följer roll och medarbetaruppdrag skulle tas fram till årsskiftet 2013/2014. En sådan riktlinje finns inte framtagen.

I samband med tillsynen gjordes, på uppdrag av objektägare patientjournal[21], en utredning kring spärrhantering för de olika system som tillhör objektfamiljen Patientjournal. Resultatet av inventeringen finns i en excelfil (daterad 2013-12-20) där 51 system listades och bedömdes enligt frågeställningarna:
- har systemet stöd för spärrhantering?
- delas informationen med annan vårdgivare?
- delas informationen med annan vårdenhet?
- finns behov att utveckla spärrhantering?
Vad gäller den sista frågan fanns det vid inventeringstillfället åtta system där det fanns behov av att utveckla spärrhanteringen samt femton system där behovet var oklart. Det framgår inte var ansvaret för det fortsatta arbetet med denna kartläggning ligger.

Landstingsdirektören har fastställt en riktlinje, *Åtkomst till patientuppgifter för hälso- och sjukvårdspersonal*[22]. Syftet med riktlinjen är att närmare klargöra vad som är tillåten respektive otillåten åtkomst till journalsystem. Dokumentet innehåller dryga 20-talet vanliga frågor och svar kring tillämpning av lag och föreskrift. Detta dokument anses vara till stor hjälp i verksamheten.

I ett PM[23], *Information ang. rutin för spärr i vårdinformationssystem*, tydliggörs regelverk och patientens rätt att begära såväl inre som yttre spärr d v s rätten att

[17] Riktlinje, giltighetstid 2013-10-31—2015-12-31
[18] Instruktion, giltighetstid 2013-08-27—2015-08-26
[19] LK/131877, Tillsyn rörande patientdatalagen, 2013-10-29
[20] Datainspektionen är en myndighet som genom sin tillsynsverksamhet ska bidra till att behandlingen av personuppgifter inte leder till otillbörliga intrång i enskilda individers personliga integritet.
[21] Objektfamilj patientjournal omfattar ca 60 system varav Cosmic, system för kliniskt vårdstöd och patientadministration, är det mest centrala i landstingets vårdverksamhet. Enligt landstingets modell för systemförvaltning finns en objektägare knuten till varje objektfamilj.
[22] Riktlinje, giltighetstid 2014-06-19—2017-06-19
[23] 2012-09-20

begränsa åtkomst av information för andra verksamhetsområden (inre spärr) och/eller för andra vårdgivare (yttre spärr). Landstinget har förutom denna information till personalen också ett informationsmaterial till patienter, *Spärrar – Om att spärra din patientjournal*.

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 riktlinjerna för informationssäkerhet anges att ”säkerhetskopiering av information och programvara ska utföras regelbundet, med frekvens och omfattning anpassad till verksamhets- respektive legala krav, enligt fastställd instruktion.” Riktlinjen hänvisar också till *Riktlinjer och regler för IT-säkerhet*[24]. I dessa riktlinjer anges att ”intervaller för säkerhetskopieringen bestäms utifrån systemägarens krav på informationens aktualitet vid återstart från en säkerhetskopia. Det är systemägaren[25] som tillsammans med driftsansvariga fastställer dessa regler i driftsinstruktionen”. Nuvarande backuprutiner för journalsystemet COSMIC anses inte vara tillfredsställande dokumenterade.

3.4.2 Bedömning

- Landstinget har sedan föregående granskning gjort flera insatser som förbättrat efterlevnaden av kraven kring behörighetstilldelning. Vi konstaterar att Datainspektionen inte har lämnat några synpunkter på den lösning som landstinget presenterat för journalsystemet COSMIC.

- Det är en brist att inte den riktlinje för behovs- och riskanalys vid tilldelning av rättigheter som följer roll och medarbetaruppdrag är framtagen. Särskilt då det till Datainspektionen meddelats att denna riktlinje skulle vara framtagen till årsskiftet 13/14.

- Riktlinje *Åtkomst till patientuppgifter för hälso- och sjukvårdspersonal* ger goda förutsättningar för att förstå och tillämpa lagen och föreskriften avseende behörigheter.

- Det är positivt att landstinget har gjort en inventering av vilka system som har stöd för spärrhantering och för vilka det finns ett behov av att utveckla denna funktion. Det behöver dock tydliggöras vem som ansvarar för detta arbete och vem som beslutar om vilka åtgärder som ska vidtas.

- Rutiner för backuphantering för journalsystemet COSMIC behöver ses över.

[24] LK/120942
[25] Motsvaras av objektägare.

Förslag till åtgärder:

- Tydliggör vem som ansvarar för arbetet med inventering av system avseende spärr samt vem som beslutar om vilka åtgärder som ska vidtas.
- Ta fram riktlinje för behovs- och riskanalys vid tilldelning av rättigheter som följer roll och medarbetaruppdrag.
- Se över rutiner för backuphantering för journalsystemet COSMIC.

3.5 Kontroll av åtkomst – spårbarhet

Inom detta område redovisas övergripande, enligt en riskbaserad ansats, kontrollen av åtkomst till logginformation, liksom spårbarheten i denna information.

3.5.1 Iakttagelser

Vad gäller åtkomstkontroll ska vårdgivaren enligt 4 kap. 3 § PDL göra systematiska och återkommande kontroller på om någon obehörig kommer åt patientuppgifter. Detta kompletteras sedan av 2 kap. 11 § SOSFS 2008:14, där det bland annat 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.

I landstingets riktlinjer för informationssäkerhet anges: ”för att säkerställa att endast behöriga användare har åtkomst till viss information, ska åtkomst loggas och tilldelade rättigheter följas upp. Det är informationsägarens ansvar att loggning sker på samtliga verksamhetskritiska IT-system, så att det i efterhand går att följa enskilda användares aktiviteter.” Enligt uppgift följer normalt informationsägarskapet linjestrukturen. För de större övergripande vårdsystemen vilar ansvaret för informationen på landstingets verksamhetschefer. Under intervjuerna ges exempel från verksamheterna att både centrala och lokala riktlinjer för logguppföljning följs för journalsystem COSMIC. Även exempel på granskningsprotokoll ges.

Riktlinje för loggkontroll i vårdinformationssystem[26] beskriver den generella logguppföljningen som gäller för alla vårdinformationssystem. Kopplad till denna ska det finnas detaljerade anvisningar för logguppföljning för respektive vårdinforma-

[26] Giltighetstid 2013-06-03—2016-06-03

tionssystem eftersom den tekniska delen ser olika ut för varje system. Fokus har varit på anvisningar för logguppföljning för journalsystem COSMIC. För övriga system finns inte dessa anvisningar.

COSMIC är landstingets största journalsystem/vårdinformationssystem och täcker ca 90 procent av den samlade verksamheten i landstingets hälso- och sjukvård. Ett exempel på detaljerad anvisning för ett enskilt vårdinformationssystem är *Riktlinje för logghantering i Cambio COSMIC*[27]. Riktlinjen beskriver utförligt logghanteringen i COSMIC med rutiner, riskfaktorer, ansvar, befogenheter med mera. Bland annat anges att: ”för att kunna följa landstingets riktlinjer för informationssäkerhet krävs en säker behörighetssättning samt uppföljning av händelseloggar i enlighet med Datainspektionens rekommendationer. Samtliga användare i COSMIC ska tilldelas unika användaridentiteter vilka ska vara hämtade från LiV-katalogen och därmed ha unika HsaIDn[28] för att säkerställa spårbarheten”.

Det ges en samstämmig bild över följsamheten till gällande ovanstående riktlinje. Men det ges också synpunkter på att förutsättningarna för denna logguppföljning kan förbättras både via systemstöd och via en centralisering av resurser för denna uppgift.

3.5.2 Bedömning

- Det är tillfredsställande att riktlinjer för logghantering i COSMIC är framtagen. Riktlinjen ger goda förutsättningar för logghantering enligt gällande regelverk.

- Det är inte tillfredsställande att det saknas anvisningar för logguppföljning för övriga system.

Förslag till åtgärder:

- Ta fram anvisningar för logguppföljning för de system där detta saknas.

- Fortsätt det arbete som enligt uppgift pågår med att dels kartlägga eventuellt systemstöd för logguppföljning och dels se över förändrad organisation för logguppföljning.

3.6 Rutiner för journalföring

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

[27] Riktlinje, giltighetstid 2013-06-24—2016-06-24
[28] HSA är en elektronisk katalog som innehåller kvalitetssäkrade uppgifter om personer, funktioner och enheter i Sveriges kommuner och landsting samt hos privata vårdgivare

3.6.1 Iakttagelser

Enligt PDL ansvarar den som för patientjournal för sina uppgifter i journalen. Enligt föreskriften ska verksamhetschefen ansvara för uppföljning av patientuppgifternas kvalitet och ändamålsenlighet. I föreskriftens anges också att informationssäkerhetspolicyn ska säkerställa att patientuppgifter i vårdgivarens dokumentation är åtkomliga och användbara för den som är behörig.

Landstingets informationssäkerhetspolicy och riktlinjer för informationssäkerhet är framtagna för att skapa förutsättningar för detta. Till stöd för journalföring finns också tidigare kommenterade vårdgivardirektiv, *Informationshantering och journalföring i hälso-och sjukvården*. Enligt detta vårdgivaredirektiv ska det finnas riktlinjer för hur patientuppgifter ska dokumenteras i patientjournaler. Ett arbete pågår med att ta fram dessa riktlinjer. Det finns även en efterfrågan på rutinbeskrivning för hur dokumentation i journal ska ske.

Vad gäller dokumentationen i COSMIC har mallar tagits fram per verksamhetsområde. Även begrepp och regelverk för sökord är framtagna. För att säkerställa att viss information alltid loggas i journalen är vissa delar obligatoriska att fylla i. Patientens personuppgifter genereras automatiskt från folkbokföringsregistret.

Vad gäller patientdokumentation anges detta vara ett område där det finns ett utbildningsbehov sett till hur journalföring ska föras på ett ändamålsenligt och kvalitetssäkrat sätt. Det framgår att journalanteckningar kan vara av mycket varierande kvalitet och omfattning.

Det finns inte något, på övergripande nivå, etablerat arbetssätt för att kontrollera journalinnehållets kvalitet och ändamålsenlighet. Det efterfrågas stöd med att etablera ett sådant arbetssätt samt även få tillgång till resurser för detta arbete. Exempel ges på att vissa kontroller görs, antingen på förekommen anledning eller utifrån ett slumpmässigt urval. Till exempel kontrolleras hyrläkares journalanteckningar extra då omdöme ska lämnas efter avslutad tjänstgöring.

Det finns ett tydligt samband mellan informationssäkerhet och patientsäkerhet. I patientsäkerhetsberättelsen för 2013[29] framgår det att av 64 Lex Maria-anmälningar[30] utgörs den andra av de fem mest frekventa anmälningarna av brister i *dokumentation/följsamhet till vårdprogram*. Här anges att bristerna inom dokumentation framförallt handlar om avsaknad av journalanteckningar, ej dokumenterade uppgifter så som anamnes, undersökningsfynd, konsultationer, telefonsamtal och riskbedömningar, vilket medfört en begränsad spårbarhet i patientens vård och behandling. Den tredje mest frekventa anmälningen avser *informationsöverföring/samverkan* och här ges exempel på brister på

[29] LK/132196
[30] Lex Maria är en lag som innebär att ett landsting/region eller en kommun ska anmäla till Inspektionen för vård och omsorg, IVO, om en patient drabbats av eller riskerat att drabbas av en allvarlig vårdskada eller sjukdom.

informationsöverföring och/eller samverkan mellan verksamheter internt och externt som i sig medfört en fördröjning av diagnos och/eller behandling av patienten.

Sammanhållen journalföring innebär att vårdgivare under vissa förutsättningar kan få direktåtkomst till varandras elektroniska journalhandlingar och andra personuppgifter som behandlas för ändamål som rör vårddokumentation. Enligt förarbetena till 6 kap. 2 § patientdatalagen får vårdgivarna själva bestämma hur informationen ska lämnas till patienten. Det finns heller inget krav på att informationen ska ges i muntlig eller skriftlig form. Det är dock viktigt att den personuppgiftsansvarige har säkra rutiner för informationsskyldigheten eftersom denne har bevisbördan för att patienten faktiskt har fått denna obligatoriska information. När det till exempel gäller patienter som inte talar svenska bör den personuppgiftsansvarige lämpligen se till att någon översätter informationen eller att det finns informationsbroschyrer på flera språk. Enligt 6 kap. 2 § tredje stycket patientdatalagen ska informationen lämnas till patienten innan uppgifterna görs tillgängliga för andra vårdgivare. Landstinget har informerat invånarna bland annat genom utskick till hushållen.

3.6.2 Bedömning

- Det finns brister vad gäller rutiner för journalföring.
- Informationssäkerhetsarbetet och patientsäkerhetsarbetet måste integreras då brister i informationshanteringen utgör ett stort riskområde inom patientrelaterade avvikelser. Detta framgår bland annat i landstingets Lex Maria-anmälningar.
- Det är en brist att det inte finns ett etablerat arbetssätt och rutiner för att säkerställa att journalinnehållet är kvalitetssäkrat och ändamålsenligt.

Förslag till åtgärder:

- Säkerställ information och utbildning för journalförande medarbetare vad gäller ändamålsenlig journaldokumentation.
- Ta fram arbetssätt och rutiner för att säkerställa att journalinnehållet är kvalitetssäkrat och ändamålsenligt.

3.7 Incidenthantering

Inom detta område redovisas hantering och uppföljning av incidenter.

3.7.1 Iakttagelser

I landstinget finns sedan 2009 ett elektroniskt system för avvikelsehantering, AHA. Systemet ska underlätta ett systematiskt arbetssätt för avvikelsehantering. Riktlinjer och råd för avvikelsehantering har tagits fram.

Det saknas struktur och systematik för hur avvikelser inom informationssäkerhetsområdet ska registreras, klassificeras och hanteras.

Även relaterat incidenthantering syns sambandet mellan informationssäkerhet och patientsäkerhet. I landstingets patientsäkerhetsberättelse framgår att det under 2013 rapporterades totalt 1 381 patientrelaterade risker i avvikelsehanteringssystemet AHA, jämfört med 1 190 under 2012. De områden där flest risker rapporterades var i storleksordning:

1. dokumentation/journaldokumentation
2. kommunikation/informationsöverföring
3. fördröjning/provhantering
4. provhantering
5. läkemedelshantering

3.7.2 Bedömning

- Det är en brist att det saknas struktur och systematik för hur avvikelser inom informationssäkerhetsområdet ska registreras, klassificeras och hanteras.

- Det framgår av patientsäkerhetsberättelsen att informationshantering utgör ett stort riskområde inom patientrelaterade avvikelser. Detta understryker vikten av att landstingsstyrelsen bör tillse att informationssäkerhet avseende patientinformation är en naturlig del av patientsäkerhetsarbetet.

- Ovanstående bedömning bör ha påverkan på hur informations- och patientsäkerhetsarbetet organiseras.

Förslag till åtgärder:

- Säkerställ struktur och systematik för hur avvikelser inom informationssäkerhetsområdet ska registreras, klassificeras och hanteras. Identifiera vilka funktioner som är berörda av dessa avvikelser och säkerställ att dessa involveras i analys och åtgärder.

- Se till att det skapas organisatoriska förutsättningar för att patient- och informationssäkerhetsarbetet kan bedrivas på ett integrerat och effektivt sätt.

3.8 Förankring i organisationen

Inom detta område redovisas arbetet med förankring i organisationen, detta innefattar bland annat informations- och utbildningsinsatser.

3.8.1 Iakttagelser

Informations- och utbildningsinsatser avseende informationssäkerhet har genomförts samt genomförs vid behov. Den utbildning som ges för nya verksamhetschefer är ett utbildningsexempel som omnämns i positiva ordalag. Under den utbildningen ges information kring landstingets informationssäkerhetsarbete. Utbildningar kring behandling av personuppgifter har också hållits samt att landstingsjuristen bland annat har deltagit på nätverksträffar för sjuksköterskor. Utmaningen är att säkerställa att informationen når ut till och tillämpas av samtliga anställda

Utbildningar ges såväl vid spontana förfrågningar från verksamhetsrepresentanter som vid planerade tillfällen som vid introduktionsutbildningar för nyanställda respektive nya verksamhetschefer.

Det stöd som finns att få i rollen som verksamhetschef och enhetschef uppfattas som tillfredsställande. Det gäller såväl de underlag som finns publicerade på intranätet samt de centrala stödfunktioner som jurist, informationssäkerhetsansvarig med flera som bistår med råd och stöd när det efterfrågas.

Som tidigare framgått av stycke 3.6.1. finns det ett stort utbildningsbehov kopplat till journalföring.

3.8.2 Bedömning

- De insatser och den struktur för informations- och utbildningsinsatser som finns är tillfredsställande.

Förslag till åtgärder:

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

4 Bilaga 1, sammanställning av förslag till åtgärder inklusive prioritering

Prioritering av åtgärder – prioritet **HÖG**
Ta fram en handlingsplan för informationssäkerhetsarbetet enligt landstingsfullmäktiges antagna informationssäkerhetspolicy.
Se till att det skapas organisatoriska förutsättningar för att patient- och informationssäkerhetsarbetet ska kunna bedrivas på ett integrerat och effektivt sätt.
Tydliggör informationsansvariges mandat och rapporteringsvägar samt överväg informationsansvariges deltagande i KBV.
Skapa en större tydlighet i hanteringen av informationssäkerhetsärenden från LS så att det tydligt kommuniceras till linjen vilka beslut och direktiv som är tagna och förväntas åtgärdas av linjen samt vem som förväntas agera. Samma tydlighet behövs vad gäller uppföljning av åtgärder.
Säkerställ att informationssäkerhetsansvariges roll och mandat tydliggörs i framtida utformning och organisering.
Gör en översyn över vilka ytterligare grupperingar, funktioner och roller som på ett avgörande sätt är viktiga för att uppnå större samordning av informationssäkerhetsarbetet. Komplettera sedan riktlinjerna med dessa grupperingars, funktioners och rollers ansvar.
Utveckla den årliga informationssäkerhetsrapporten till att återrapportera på fler delar än de som föreskriften påbjuder. T ex kan en utgångspunkt vara att återrapportera på ytterligare områden relaterat till landstingets riktlinjer. Rapporten kan också innehålla förslag på var ansvaret för de listade förbättringsområdena bör ligga. Överväg 2 rapporteringstillfällen per år.
Färdigställ förteckningen över vilka vårdinformationssystem som innehåller patientuppgifter samt prioritera arbetet med systemavveckling.
Tydliggör vem som ansvarar för arbetet med inventering av system avseende spärr samt vem som beslutar om vilka åtgärder som ska vidtas.
Säkerställ information och utbildning för journalförande medarbetare vad gäller

ändamålsenlig journaldokumentation.
Se över rutiner för backuphantering för journalsystemet COSMIC.
Ta fram arbetssätt och rutiner för att säkerställa att journalinnehållet är kvalitetssäkrat och ändamålsenligt.
Säkerställ struktur/systematik för hur avvikelser inom informationssäkerhetsområdet ska registreras, klassificeras och hanteras. Identifiera vilka funktioner som är berörda av dessa avvikelser och säkerställ att dessa involveras i analys och åtgärder.
Ta fram anvisningar för logguppföljning för de system där detta saknas.

Prioritering av åtgärder – prioritet **MEDEL**
Utveckla den årliga informationssäkerhetsrapporten till att återrapportera på fler delar än de som föreskriften påbjuder. T ex kan en utgångspunkt vara att återrapportera på ytterligare områden relaterat till landstingets riktlinjer. Rapporten kan också innehålla förslag på var ansvaret för de listade förbättringsområdena bör ligga. Överväg 2 rapporteringstillfällen per år.
Ta fram riktlinje för behovs- och riskanalys vid tilldelning av rättigheter som följer roll och medarbetaruppdrag.
Utvärdera tillämpningen av modellen för förvaltningsstyrning avseende informationssäkerhetsperspektivet.
Tydliggör vem som ansvarar för den övergripande uppföljningen av efterlevnad av policy och riktlinjer då detta övergripande uppföljningsansvar ligger på en gruppering som inte är aktiv.
Följ upp att den information som getts till verksamhetscheferna kommer övrig personal till del på ett strukturerat sätt.

Prioritering av åtgärder – prioritet **LÅG**
Fortsätt det arbete som enligt uppgift pågår med att dels kartlägga eventuellt systemstöd för logguppföljning och dels se över förändrad organisation för logguppföljning.

5 Bilaga 2, sammanfattande redovisning av vidtagna åtgärder sedan rapport nr 5-11, Granskning av efterlevnad av patientdatalagen (2008:355)

Prioritering av åtgärder – prioritet **HÖG**	Åtgärdat ja/nej/delvis
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.	Ja
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.	Delvis, utredning avseende informationssäkerhetsansvarig pågår
Upprätta en samlad förteckning av vilka vårdinformationssystem som innehåller patientuppgifter och i vilken utsträckning de möter kraven i Patientdatalagen och föreskrift 2008:14	Delvis
Utred snarast orsakerna till varför det finns brister i åtkomst till patientinformation samt hur dessa ska åtgärdas.	Ja
Genomför en riktad informationsinsats till samtlig personal, även de inom administrativa enheter, rörande Patientdatalagen och föreskrift 2008:14. Komplettera med informationsmaterial.	Delvis, pågående arbete

Prioritering av åtgärder – prioritet **MEDEL**	Åtgärdat ja/nej/delvis
Säkerställ att informationssäkerhetsansvarigs organisatoriska tillhörighet till Landstings-IT *inte* innebär att ansvaret att styra och ställa krav på informationssäkerheten läggs på IT-avdelningen.	Sedan föregående granskning har informationssäkerhetsansvarig tillhört HS-staben. Utredning pågår kring utformning av framtida roll och or-

	ganisering
Ta fram skriftlig dokumentation som tydligt beskriver vilket ansvar vårdgivaren har lagt på verksamhetschefen.	Ja
Säkerställ att verksamhetscheferna tar fram, fastställer och dokumenterar ändamålsenliga rutiner för informationshanteringen.	Delvis
Revidera *Informationshandboken*. Säkerställ att *Informationshandboken* beaktar Personuppgiftslagen. Skapa en rutin för att kontinuerlig följa upp och revidera denna handbok.	Informationssäkerhetshandboken är ersatt av informationssäkerhetspolicy
Säkerställ att det görs en behovs- och riskanalys inför tilldelning och kontinuerlig uppföljning av behörigheter på samtliga vårdsystem.	Delvis
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.	Ja
Vidga *Övergripande regelverk vid logguppföljning* till att omfatta samtliga vårdinformationssystem. Utforma rutiner för uppföljning för att säkerställa regelverkets efterlevnad.	Ja
Revidera dokument *Riktlinjer för logghantering i COSMIC*. Utforma rutiner för uppföljning för att säkerställa riktlinjernas efterlevnad.	Ja
Säkerställ att avvikelser klassificeras på ett sätt som möjliggör utdata där ärenden som avser brister i informationssäkerheten relaterat lag och föreskrift går att identifiera.	Nej
Identifiera vilka funktioner som är berörda av dessa avvikelser och säkerställ att dessa involveras i analys och åtgärder.	Nej
Följ upp och säkerställ att den information som givits verksamhetscheferna kommer övrig personal till del på ett strukturerat sätt.	Delvis

Prioritering av åtgärder – prioritet **LÅG**	Åtgärdat ja/nej/delvis
Revidera omgående dokument *Riktlinje för tillgång till vårdinformationssystem för hälso- och sjukvårdspersonal* så att den följer och refererar	Ja

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.	Ja

6 Bilaga 3, intervjupersoner

Följande personer är intervjuade: Landstingsdirektör, en av landstingets två hälso- och sjukvårdschefer, chefläkare och tillika processägare patientsäkerhet, verksamhetschef och chefssekreterare njurmedicinska kliniken, verksamhetschef och enhetschef allmänmedicin, informationssäkerhetsansvarig, landstingsjurist samt objektägare patientjournal.

Via telefon har även information inhämtats från landstingsarkivarie (tillika personuppgiftsombud) samt från enhetschef ledningsstöd.

7 Bilaga 4, Erhållna dokument

Granskning: Informationssäkerhet Patientinformation LiV			
Underlag: Erhållna dokument			
Dokumenttyp	**Antagen/fastställd**	**Giltig t.o.m.**	**Dokumentägare**
1, Policy - Informationssäkerhetspolicy	2012-11-28 av LFM	2015-11-28	Eije Berneflo
2, Riktlinje - Tillgång till patientuppgifter för hälso- och sjukvårdpersonal.	2014-06-19 av LD	2017-06-19	Eije Berneflo, Isabelle Edgren
4, Riktlinje - Riktlinje för loggkontroll i vårdinformationssystem	2013-06-03 av LD	2016-06-03	Informationssäkerhetsfunktionen
5, Riktlinje - Informationssäkerhet	2012-11-28 av Hans Karlsson	2015-11-28	Eije Berneflo
6, Riktlinje/manual - Riskanalysmanual	Till LDL 2012-04-30	Framgår ej, tills vidare?	Utfärdad av Eije Berneflo och Håkan Nilsson, Göran Karlström
7, Riktlinje - Hantering av skyddade personuppgifter inom hälso- och sjukvården samt tandvården	2013-01-01	2015-12-31	Maj-Britt Andersson
8, Yttrande över revisorernas granskningsrapport	2012-02-21		Eije Berneflo, handläggare
9, Riktlinje - Utlämnande av journalhandlingar	2012-11-01 av Hans Karlsson	2015-10-31	Isabelle Jacobson
10, Vårdgivardirektiv - Informationhantering och journalföring i hälso- och sjukvår-	2014-01-01 av LS	2016-12-31	Samordningsansvarig för vårdgivardirektiv

den			
11, Handlingsplan för att uppfylla patient-datalagen samt socialstyrelsens föreskrift SOSFS 2008:14.	Delrapport	Pågående arbete	Eije Berneflo, handläggare
12, Information ang. rutin för spärr i vårdinformationssystem	PM 2012-09-20	Gäller	Eije Berneflo
13, Spärrar - folder. Information till patient om hur spärra sin journal.	Framgår ej.	Gäller	Eije Berneflo
14, Riktlinje för logghantering i Cambio COSMIC	2013-06-24	2016-06-24	Göran Karlström
15, Översikt till konfigurationshanteringen i Sharepoint	Mall, ej daterad.		PUO
16, PUL-applikation	Lista uttagen från intranät? 2014-08-29, http://pul.liv.se/ala-register.aspx?		Framgår ej.
17, Konfigurationshantering	Lista uttagen från intranät? 2014-08-29, http://ea.liv./CMDB/_layouts/15/start.aspx		Framgår ej.
18, Rutin - Remisshantering god praxis rutin	2013-12-01 Hälso- och sjukvårdschef	2015-12-31	Stabschef Hälso- och sjukvårds-staben
19, Granskningsprotokoll 2014/loggkontroll Cosmic			
20, Rutiner vid begäran om journalkopior och utdrag av personupppgiftsbehandling-ar	2011-12-01 - Landstingsarkivarie Hans Ramstedt	41973	Landstingsarkivarie Hans Rams-tedt
21, Skyddade personuppgifter riktlinjer	2013-01-01 - Hälso- och sjukvårdschefen	2015-12-31	Maj-Britt Andersson
22, rutin för inkommande svar vid läkares frånvaro	2013-09-23 Anders Olsson	41608	Irene Malmkvist
23, Bild över - Organisation för patiensä-kerhetsarbete			
24, Information från tjänsteman - Uppdrag strategisk patientsäkerhetsgrupp			
25, Information från chefläkare - Planering rapport av kvalitetsindikatorer			
26, Information från chefläkare - Patient-säkerhet slutversion			
27, Information från chefläkare - Delta-gande funktioner I DEN STRATEGISKA PATIENTSÄKERHETSGRUPPEN			
28, Information från chefläkare - Tertial-rapport			
29, Rutin - Logghantering Cosmic	2014-01-01, Karin Malmkvist	2015-12-31	Karin Malmqvist
30, Rutin för praktisk tillämpning av Messenger	2014-06-18, Karin Malmkvist	2017-06-17	Cosmicgruppen i Allmänmedicin
31, Instruktion - Medicinsk kvalitetskon-troll inhyrda läkare	2014-03-01, Karin Malmkvist	2015-12-31	Karin Malmqvist
32, Cosmic allmän medicin skärmdumpar			
33, Befattningsbeskrivning samordnare Cosmic inom allmän medicin			
34, Förslag övergripande loggrutin njur-medicin	Divisionschef medicinska specialister		Verksamhetschefer inom divis-ionen
35, Informationssäkerhetsrapport 2013	Tjänsteskrivelse 2014-03-25		
36,Förvaltningsmodell för leddningssystem central			Enheten för ledningsstöd

37, Kommunikation, veta,känna, göra om ledningssystem			Enheten för ledningsstöd
38, Presentation av "Vårt arbetssätt"			Enheten för ledningsstöd
39, Information om ledningssytem "Vårt arbetssätt"			Enheten för ledningsstöd
40, Övergripande bild av ledningssytemet			Enheten för ledningsstöd
41, Bild, resultatet av ledningssystemet			Enheten för ledningsstöd
42, Anställningsavtal verksamhetschef			
43, Bilaga - Verksamhetschefens medicinrättsliga ansvar			
44, Instruktion - Behörighetsprofiler COSMIC	Göran Karlström 2013-08-27	2015-08-26	Gun De Vahl
45, Rutin - Behörighetstilldelning, tillgång till vårddata i COSMIC	Göran Karlström 2013-10-31	2015- 12-31	Katarina Hallgren
46, Delegeringsordning för landstingsstyrelsen	Landstingsstyrelsen	2014-09-23	Anna-Lena Wingqvist
47, Datainspektionen tillsyn		2013-10-29	Eije Bernflo
48, Datainspektionen tillsyn tjänsteskrivelse			Eije Bernflo
49, Förteckning över system med vårddokumentation som avses i 2 kap. 4 § 1 och 2 PDL	Isabelle Jacobsson 2012-02-02		
50, Tillsyn PDL DI	2013-10-15		
51, Logghantering i Cosmic	2012-02-08, godkänd av Claus Vigsö	2015-02-07	Divisionschef för psykiatri
52, Landstingets protokoll	2012-05-29		
53, PM - Objektägare för system	2014-09-25		
54, Organisationsskiss tjänstemannaledning			
55, Patiensäkerhetsberättelse 2013	Fastställd av LF 2014-04-29		
56, Riktlinje för logghantering i Cambio COSMIC	2013-06-24, fastställd av Göran Karlström	2016-06-24	Göran Karlström
58, Riktlinjer för tillgång till vårdinformation	Fastställda av LS 2007-10-16		
59, Riktlinje - IT-säkerhet			Håkan Nilsson
60, Riskanalysmall			
61, Riskanalysmanual LiV	2012-03-13 Eije Berneflo, Håkan Nilsson		
62, SOSFS 1997:8 Socialstyrelsens allmänna råd; Verksamhetschef inom hälso- och sjukvård			
63, Uppdrag och ansvar för verksamhetschef			
64, Utredning spärrhantering patientjournal			
65, Riktlinje styrande dokument	Hans Karlsson 2013-06-20	2014-06-20	Matilda Eng

2014-11-18

_____

Eva Lidmark, uppdragsledare