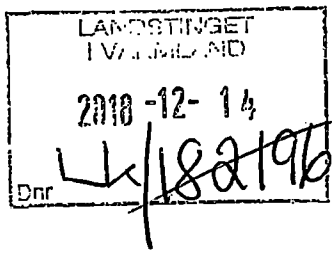
Landstinget i Värmland

REVISORERNA
Handläggare
Johan Magnusson

Direkttelefon
054-61 40 60

Datum
2018-12-10
Ert datum

Vår beteckning
Rev/18023
Er beteckning



RS/190202

Landstingsstyrelsen (för kännedom)

Informationssäkerhet – patientinformation - uppföljning

Landstingets revisorer ansvarar för att genomföra årlig granskning av landstingets samtliga verksamheter. Utifrån detta uppdrag och ansvar har landstingets revisorer utarbetat och dokumenterat en "Granskningsstrategi". Baserad på granskningsstrategin gör revisorerna årligen en riskbedömning och revisionsplan. I dokumentet "Revisionsplan 2018" ingår bland annat en uppföljande granskning avseende informationssäkerhet - patientinformation.

Landstingets revisorer genomförde en uppföljande granskning avseende informationssäkerhet – patientinformation år 2014.

Av revisorernas bedömning i ovan nämnda granskning framgick bland annat att landstingsstyrelsen tillsett att vissa av de förbättringsåtgärder som föreslogs i revisorernas rapport från 2011 hade genomförts. Den viktigaste åtgärden var framtagande av Informationssäkerhetspolicy och Riktlinje för informationssäkerhet. Granskningen visade dock att det fanns ytterligare åtgärder som behövde vidtas:

Tätare och mer utförlig återrapportering till landstingsstyrelsen borde ha skett för att säkerställa att planerade åtgärder vidtagits.

Den informationssäkerhetsrapport som landstingsstyrelsen får årligen kan förbättras sett till frekvens och utvidgning av innehåll.

Frånvaron av en fastställd handlingsplan för informationssäkerhetsarbetet var dock ett avsteg från den av landstingsfullmäktige antagna informationssäkerhetspolicyn.

Bedömningen var att landstinget i högre grad - än vid det tidigare granskningstillfället 2011 - efterlevde patientdatalagen med tillhörande föreskrifter.

Postadress
Landstinget i Värmland
Landstingshuset
651 82 Karlstad

Besöksadress
Rosenborgsgatan 50

Telefon (växel)
054 61 50 00
Telefax

E-postadress
johan.magnusson@liv.se
Org.nr
232100-0156

Syftet med den nu aktuella uppföljningen har varit att granska vilka åtgärder landstingsstyrelsen vidtagit för att säkerställa en ändamålsenlig informationssäkerhet rörande patientinformation. Granskningen har haft sin utgångspunkt i de synpunkter och förbättringsförslag som redovisades i revisorernas rapport från 2014.

För att säkerställa helhetsgreppet inom området säkerhet har landstingsstyrelsen antagit en ny Säkerhetsstrategi i vilken informationssäkerhet utgör en del. Säkerhetsstrategin har ersatt den tidigare Informationssäkerhetspolicyn. Det har också gjorts en översyn av övriga befintliga dokument och vid behov har dessa reviderats. Dessutom har nya dokument utarbetats.

Landstingsstyrelsens har beslutat att ett regionalt säkerhetsråd tillskapas, i enlighet med Säkerhetsstrategin.

Landstingsstyrelsen har fastställt en organisation för patient- och informationssäkerhetsarbetet. I beslutet förtydligades att ansvaret för informationssäkerhetsarbetet följer linjeorganisationen.

Sedan tidigare fanns ett beslut om att inrätta ett så kallat informationssäkerhetsråd.

Landstingsstyrelsen har också beslutat att utse två Informationssäkerhetssamordnare på övergripande nivå. Detta är delvis en ny funktion då den tidigare funktionen som informationssäkerhetsansvarig ändras till en roll där huvudfokus ligger på att föreslå nödvändiga styrande ledningsdokument inom organisationen. Ytterligare en uppgift för Informationssäkerhetssamordnarna är att följa upp, utvärdera och redovisa informationssäkerhetsarbetet på övergripande nivå.

Vi har i denna uppföljande granskning konstaterat att landstingsstyrelsen vidtagit åtgärder, bland annat med anledning av de iakttagelser och rekommendationer som revisorerna framförde i sin uppföljande granskning år 2014. Vissa åtgärder har också vidtagits med anledning av förändringar i lagstiftning och föreskrifter.

Sammanfattningsvis är bedömningen att vidtagna åtgärder och pågående utvecklingsarbete i stort överensstämmer med de rekommendationer som revisorerna framförde i sin uppföljande granskning år 2014.

Landstingets revisorer översänder härmed rapporten för kännedom.

Östen Högman
ordförande

Daniel Bergqvist
vice ordförande

LANDSTINGET I VÄRMLAND
Revisionskontoret
Johan Magnusson

Rev/18023

2018-12-10

Informationssäkerhet – patientinformation – uppföljning

Rapport 15-18

Informationssäkerhet - patientinformation – uppföljning

Bakgrund

Landstingets revisorer ansvarar för att genomföra årlig granskning av landstingets samtliga verksamheter. Utifrån detta uppdrag och ansvar har landstingets revisorer utarbetat dokumentet "Granskningsstrategi" i vilket de beskrivit de områden som revisorerna främst ska fokusera på under innevarande mandatperiod. Baserad på granskningsstrategin gör revisorerna en årlig "Riskbedömning och revisionsplan". I "Revisionsplan 2018" ingår bland annat en uppföljande granskning till den granskning avseende "Informationssäkerhet – patientinformation" som genomfördes år 2014.

Granskningen som genomfördes år 2014 var en uppföljning av en granskning som genomfördes år 2011 (nr 5 - 11).

Den granskning som genomfördes år 2014 utgick från följande frågeställningar:

- Har landstingsstyrelsen sett till att genomföra de förbättringsåtgärder som föreslås i granskningsrapporten?

- Har landstingsstyrelsen fått en kontinuerlig återapportering av genomförda åtgärder i enlighet med landstingsstyrelsens 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 2014 genomfördes med hjälp av konsultstöd. I konsulternas rapport redovisades iakttagelser avseende samtliga revisionsfrågor i granskningen. Konsulten framförde också förslag till åtgärder i rapporten.

Syfte, revisionsfrågor

Syftet med denna uppföljning är att granska vilka åtgärder landstingsstyrelsen vidtagit för att säkerställa en ändamålsenlig informationssäkerhet rörande patientinformation. Granskningen ska ta sin utgångspunkt i de synpunkter och förbättringsförslag som redovisades i revisorernas rapport från 2014.

Denna uppföljande granskning ska ge svar på följande revisionsfråga:

- Har landstingsstyrelsen vidtagit åtgärder med anledning av de brister samt de förbättringsförslag som framfördes i granskningsrapporten 2014?

Avgränsning

Uppföljningen har avgränsats till att gälla informationssäkerhet inom Landstinget i Värmland 2018 samt uppföljning av den granskning som genomfördes år 2014.

Revisionskriterier

Uppföljningen har skett utifrån aktuell lagstiftning och föreskrifter inom området. Revisionskriterier är också fullmäktiges beslut samt landstingsstyrelsens reglemente.

Ansvarig nämnd

Landstingsstyrelsen är ansvarig nämnd.

Metod

Uppföljningen har genomförts genom dokumentstudier och intervjuer. Intervjuer har genomförts med landstingets informationssäkerhetssamordnare samt den jurist som är knuten till Informationssäkerhetsrådet.

Rapporten är faktakontrollerad av de som intervjuats samt kvalitetssäkrad av landstingets revisionschef.

Granskningens resultat

Utgångspunkten och upplägget i den aktuella rapportenen bygger på den granskning som genomfördes år 2014.

Iakttagelser i den uppföljande granskning som genomfördes 2014

I den uppföljande granskning som revisorerna lät genomföra 2014 var bedömningen att de förbättringsåtgärder som föreslogs i revisorernas rapport från 2011 till vissa delar hade genomförts. Den viktigaste åtgärden var framtagande av Informationssäkerhetspolicy och Riktlinje för informationssäkerhet. Granskningen visade att det fanns ytterligare åtgärder som behövde vidtas.

I uppföljningen konstaterades att landstingsstyrelsen vid ett tillfälle fått återrapportering av genomförda åtgärder och att ytterligare avrapportering borde ha skett för att säkerställa att planerade åtgärder vidtagits.

Landstingsstyrelsen får årligen en informationssäkerhetsrapport som följer Socialstyrelsens föreskrift avseende kraven på innehåll. Bedömningen var att denna återrapportering kan förbättras sett till frekvens och utvidgning av innehåll.

Genom upprättande av informationssäkerhetspolicy och riktlinjer för informationssäkerhet hade landstingsstyrelsen förbättrat förutsättningarna för styrning, uppföljning och intern kontroll och efterlever i större utsträckning än vid granskningstillfället (2011) gällande bestämmelser. Frånvaron av en fastställd handlingsplan för informationssäkerhetsarbetet är dock ett avsteg från den av landstingsfullmäktige antagna informationssäkerhetspolicyn.

Bedömningen var att landstinget i högre grad - än vid granskningstillfället 2011 - efterlevde patientdatalagen med tillhörande föreskrifter.

Förbättringsförslag och rekommendationer i 2014 års granskning

Den sammanfattande bedömningen var som nämnts ovan att det kvarstod ett antal brister och en samlad förteckning över förslag till förbättringar redovisades i rapportens bilaga. Antalet förbättringsförslag var stort och de var av varierande slag och omfattning. Rekommendationerna var av såväl administrativ som teknisk art.

Bland de förbättringsförslag och rekommendationer som lämnades i granskningen 2014 kan nämnas: att det tas fram en handlingsplan för informationssäkerhetsarbetet enligt fastställd informationssäkerhetspolicy, att det skapas organisatoriska förutsättningar för patient- och informationssäkerhetsarbetet samt att informationssäkerhetsansvariges roll och mandat tydliggörs.

Landstingsstyrelsens svar

Rapporten översändes till Landstingsstyrelsen som i sitt svar till revisorerna (LK/142762) framförde följande:

Landstingsstyrelsen angav att landstinget för närvarande saknar informationssäkerhetssamordnare men att ett rekryteringsarbete inletts. Informationssäkerhetssamordnaren fungerar normalt även som informationssäkerhetsansvarig. Tills det att ny informationssäkerhetssamordnare rekryterats har styrelsen utsett en av landstingsjuristerna som tillförordnad informationssäkerhetsansvarig.

Landstingsstyrelsen framhöll i sitt svar att ett arbete hade gjorts i syfte att skapa tydligare uppdrag och organisatoriska förutsättningar för informationssäkerhetssamordnaren. Framtagandet av en handlingsplan för informationssäkerhetsarbetet blir en prioriterad uppgift för den som tillträder uppdraget.

Landstingsstyrelsen påpekade att den tillträdande informationssäkerhetssamordnaren också kommer ha ett viktigt uppdrag att forma organisationen kring informationssäkerhetsarbetet. Styrelsen pekade bland annat på att den strategiska gruppen för informationssäkerhet bör återupprättas. Gruppens sammansättning ska ge förutsättningar att integrera patient- och informationssäkerhetsarbetet samt i övrigt verka för en bra samordning av informationssäkerhetsarbetet.

Svar på revisionsfrågor

Aktuella iakttagelser/bedömningar

Nedan redovisas de iakttagelser som gjorts i den nu aktuella uppföljande granskningen. Den aktuella revisionsfrågan i granskningen är:

Har landstingsstyrelsen vidtagit åtgärder med anledning av de brister samt de förbättringsförslag som framfördes i granskningsrapporten 2014?

Utifrån de iakttagelser och förbättringsförslag har följande nedbrutna revisionsfrågor (kursiverade) formulerats:

Har det utarbetats en handlingsplan för informationssäkerhetsarbetet i enlighet med fastställd informationssäkerhetspolicy?

Landstinget har ett antal olika styrande dokument som avser säkerhet, inom olika områden och på olika nivåer inom organisationen. Landstingsstyrelsen har, för att styrning och ledning inom säkerhetsområdet

ska bli tydligare och effektivare, sett över och vid behov reviderat befintliga dokument och utarbetat nya dokument. För att säkerställa helhetsgreppet inom området har en övergripande säkerhetsstrategi utarbetats i vilken informationssäkerhet utgör en del. Vid landstingsstyrelsens möte 2018-02-20 godkändes förslag till Säkerhetsstrategi och styrelsen beslutade även att ett regionalt säkerhetsråd tillskapas, i enlighet med säkerhetsstrategin.

Säkerhetsstrategin är överordnad de riktlinjer som finns idag inom olika säkerhetsområden. En förutsättning för ett fungerande säkerhetsarbete är att riktlinjerna även kompletteras med rutiner, interna instruktioner och checklistor inom respektive verksamhet samt att dessa sedan implementeras och används i det dagliga arbetet.

Den nyligen beslutade övergripande Säkerhetsstrategin har som nämnts ovan ersatt den tidigare Informationssäkerhetspolicyn. En handlingsplan har ännu ej upprättats. I samband med denna granskning har framkommit att arbete pågår för att upprätta en handlingsplan utifrån den Säkerhetsstrategi som landstingsstyrelsen beslutade godkänna i februari 2018.

Hur ser de aktuella organisatoriska förutsättningarna, för patient- och informationssäkerhetsarbetet, ut?

Landstingsstyrelsen har vid sitt möte 2018-05-22 fastställt en organisation för patient- och informationssäkerhetsarbetet. I beslutet förtydligades att ansvaret för informationssäkerhetsarbetet följer linjeorganisationen.

För att koordinera arbetet fanns sedan tidigare beslut om att inrätta ett så kallat informationssäkerhetsråd där representanter för verksamheter, PM^3-organisationen* samt specialister såsom informationssäkerhetssamordnare, IT-säkerhetsansvariga, jurister m.fl. ingår.

Landstingsstyrelsen beslutade också vid mötet 2018-05-22 att utse två namngivna personer som Informationssäkerhetssamordnare på övergripande nivå. Detta är delvis en ny funktion då den tidigare funktionen som informationssäkerhetsansvarig ändras till en roll där huvudfokus ligger på att föreslå nödvändiga styrande ledningsdokument inom organisationen. Ytterligare en uppgift för Informationssäkerhetssamordnarna är att följa upp, utvärdera och redovisa informationssäkerhetsarbetet på övergripande nivå. Uppgiften som rör förteckning av personuppgiftsbehandling övertas av den övergripande informationssäkerhetssamordnaren då rollen som personuppgiftsombud (PUO) försvinner.

En av de två informationssäkerhetssamordnarna har en uttalad roll som informationssäkerhetssamordnare med fokus på hälso- och sjukvården. Detta är i överensstämmelse med de krav som anges i HSLF-FS 2016:40 om journalföring och behandling av personuppgifter i hälso- och sjukvården.

När det gäller övriga funktioner som är delaktiga i landstingets informationssäkerhetsarbete finns IT-säkerhetsansvarig samt säkerhetssamordnare etablerade inom organisationen.

I samband med denna uppföljande granskning berördes även vissa nya utmaningar avseende patient- och informationssäkerhet som är aktuella inom hälso- och sjukvården. Bland annat berördes bytet av it-stöd från Meddix SVP (it-stöd som används av kommuner, landsting och privata vårdgivare för meddelandehantering i samband med vårdplanering vid utskrivning från slutenvård) till COSMIC Link (motsvarande funktion som Meddix) samt de nya web-baserade aktörer inom hälso- och sjukvården som etablerats (KRY, Netdoktor m.fl.).

Har den informationssäkerhetsansvariges roll och mandat tydliggjorts?

Som nämnts ovan har funktionen informationssäkerhetsansvarig ersatts av två informationssäkerhetssamordnare på övergripande nivå. Deras roll

* PM^3 är en styrmodell som utvecklats för verksamhetsutveckling samt för styrning och uppföljning av en organisations hela uppdragsportfölj.

och mandat är av rådgivande och normerande karaktär. Enligt landstingsstyrelsebeslut 2018-05-22 följer ansvaret för informationssäkerhet linjeorganisationen och ansvaret ligger följaktligen på verksamhetscheferna.

Vilka övriga åtgärder har vidtagits med anledning av de rekommendationer som lämnades i rapporten från 2014?

Sedan den föregående granskningen har styrande dokument setts över och i vissa fall kompletterats. Landstingsstyrelsen har, som beskrivits ovan, fastställt Säkerhetsstrategin där informationssäkerhet utgör en del. Det pågår arbete med att ta fram en ny riktlinje för informationssäkerhet. I ärendehanteringssystemet VIDA finns rutiner avseende informationssäkerhet tillgängliga. Verksamhetsanpassade instruktioner avseende informationssäkerhet finns framtagna.

Sammanfattande bedömning och rekommendationer

Vi har i denna uppföljande granskning konstaterat att landstingsstyrelsen vidtagit åtgärder, bland annat med anledning av de iakttagelser och rekommendationer som revisorerna framförde i sin uppföljande granskning år 2014. Vissa åtgärder har också vidtagits med anledning av förändringar i lagstiftning och föreskrifter.

Sammanfattningsvis är bedömningen att vidtagna åtgärder och pågående utvecklingsarbete i stort överensstämmer med de rekommendationer som revisorerna framförde i sin uppföljande granskning år 2014.

Johan Magnusson
Certifierad kommunal yrkesrevisor