www.pwc.se

Revisionsrapport

Granskning av säkerhet i patientsystemet och hantering av patientjournaler

Region Västmanland

Mikael Grönvik
Lina Zhou

Maj 2018

pwc

Innehåll

Sammanfattning

Patientdatalagen (2008:355) syftar till att säkerställa att patientjournal förs för varje enskild patient vid varje specifikt vårdtillfälle. Patientdatalagen (2008:355) reglerar även vem som anses behörig av patientjournalens innehåll och att vårdanställda endast ska kunna ta del av uppgifter som behövs för att de ska kunna utföra sina arbetsuppgifter.

Hur säkerställer regionstyrelsen en god säkerhet i patientsystemet och hanteringen av patientjournaler?

Vi grundar vår bedömning på den avstämning av kontrollmål, som ligger till grund för att svara på revisionsfrågan, som har gjorts genom intervjuer och stickprovsgranskning. Vi bedömer att regionstyrelsen för Region Västmanland delvis har en god säkerhet i patientsystemet (Cosmic) och hantering av patientjournaler, men vi har uppmärksammat ett antal brister som måste ses över. Regionen har en robust IT-miljö för att hantera avbrott och driftstopp, dock finns det en viss avsaknad av processer och rutiner för att kontrollera essentiella uppgifter:

- Inloggningen i Cosmic kan ske på två sätt varav den ena inte uppfyller kraven på stark autentisering.
- Det existerar ingen process för att kontinuerligt utföra stickprov på behörigheterna i patientjournalsystemet, vilket försvårar för vårdgivaren att kunna säkerställa att användaren har rätt behörighet i Cosmic
- Det finns en god teknisk säkerhet av journalsystemet dock finns det brister med inloggningen till Cosmic.
- Det finns inga erforderliga processer på plats som säkerställer att användare har korrekt behörighet i Cosmic.

Utöver de ovan nämnda brister har regionen bra kontroll över hanteringen av loggarna som genereras av journalsystemet och uppfyller de kraven som finns i HSLF-FS 2016:40:

- Loggarna för journalsystemet finns både i Cosmic och i LoggKoll. Analys av loggarna sker vanligtvis direkt i LoggKoll av verksamhetschefen eller av utsedda loggranskare.
- Det finns en tydlig ansvarsfördelning avseende loggarna på både centralnivå och på verksamhetsnivå. Återkommande kontroller av loggarna sker månatligen

1. Inledning

1.1. Bakgrund

Patientdatalagen (2008:355) syftar till att säkerställa att patientjournal förs för varje enskild patient vid varje specifikt vårdtillfälle. Patientjournalen ska alltid innehålla obligatoriska uppgifter som bevaras minst tio år. Enligt lagen har patienten själv samt behöriga rätt att få tillgång till journalen. Patientdatalagen (2008:355) reglerar även vem som anses behörig av patientjournalens innehåll.

För att kontrollera riktlinjerna för vad som är obehörig åtkomst inledde datainspektionen (DI), år 2013, en granskning av samtliga landsting och regioner. Anledningen till granskningen var att 52 anställda i landsting och regioner hade polisanmälts för dataintrång under 2012. Enligt patientdatalagen (2008:355) ska vårdanställda endast kunna ta del av uppgifter som behövs för att de ska kunna utföra sina arbetsuppgifter.

Region Västmanland har utifrån väsentlighet och risk beslutat att granska säkerheten kring journalsystemet Cosmic, utifrån förebyggande insatser, behörigheter och kontroller.

1.2. Syfte och Revisionsfråga

Hur säkerställer regionstyrelsen en god säkerhet i patientsystemet och hanteringen av patientjournaler?

1.3. Revisionskriterier

Patientdatalagen (2008:355)

Socialstyrelsens föreskrifter och allmänna råd (HSLF-FS 2016:40) om journalföring och

behandling av personuppgifter i hälso- och sjukvården

Regionens riktlinjer för patientinformation och journalhantering

1.4. Kontrollmål

Granskningen inriktats mot följande kontrollfrågor:

- Finns det kontroller avseende intrång?
- Finns process för att kontinuerligt utföra stickprov på behörigheterna i patientjournalsystemet?
- Är den tekniska säkerheten av journalsystemet på en tillfredställande nivå?
- Finns erforderliga processer på plats för att säkerställa behörigheterna i patientjournalsystemet?

- Finns det specifika loggar och en process för att analysera dessa?
- Finns det ett tydligt ansvar för loggarna och kontroll av dessa?

1.5. Avgränsning

Granskningen avser regionstyrelsens övergripande ansvar.

1.6. Metod

Granskningen omfattar intervjuer med ansvariga chefer och tjänstemän såsom verksamhetschefer, enhetschefer, systemförvaltare, användare och superusers. Fullständig lista finns i Bilaga 1.

Granskning av säkerheten journalsystemet Cosmic och gällande riktlinjer/rutiner och övrig relevant dokumentation. Verifiering av regionens egna kontroller och kontroll av loggsystem. Granskade dokument finns i Bilaga 2.

2. Granskningsresultat

För varje kontrollmål redogörs för vilka iakttagelser och revisionella bedömningar som gjorts.

2.1. Finns det kontroller avseende intrång?

2.1.1. Utgångspunkt

Enligt 4 Kap. 3 § i Patientdatalagen (PDL) ska åtkomstkontroller göras för att säkerställa att användare inte använder sina behörigheter på fel sätt genom att läsa, ändra eller ta bort information som de inte ska behandla. Det kan exempel vara när en användare på en felaktig åtkomst tittar i en patientjournal trots att han eller hon inte deltar i vården av patienten eller av annat skäl inte behöver uppgiften för sitt arbete inom hälso- och sjukvården.

Enligt 6 kap. 1 § HSLF-FS 2016:40 ska hälso- och sjukvårdspersonalen ansvara för att personliga lösenord och hjälpmedel för autentisering inte ska bli tillgängliga för annan.

2.1.2. Iakttagelser

Intrång kan beaktas på två sätt: intrång av anställda och externt intrång. Nedan redogörs båda delarna.

Intrång av anställda

Samtliga användare har en viss behörighet och därmed olika nivåer av åtkomst i journalsystemet. Baserad på intervjuerna framkom det att det finns två olika sätt att logga in i journalsystemet, 1) SITHS-kort 2) lösenord

SITHS-kortet är det verktyg för att uppfylla kraven på stark autentisering där en persons identitet kontrolleras med tvåfaktorsautentisering. Vid inloggning i Cosmic med SITHS-kort måste kortet dockas i för första identifiering och sedan en personlig pinkod som steg två. Våra iakttagelser som är baserad på intervjuerna tyder på att användare väljer medvetet bort alternativet med att logga in med SIHTS-kort av den anledningen att kortet även används som passerkort, vilket försvårar arbetet i Cosmic eftersom kortet måste sitta i.

Lösenordet som används för att komma in i journalsystemet i Region Västmanland är samma lösenord som användaren fått tilldelat till sig vid sin anställning. Det kan förekomma vid enstaka fall att användaren ändrar lösenordet, som sker i samband vid misstanke av intrång. Det förekommer en risk att en obehörig kan få åtkomst till inloggningsuppgifter för en eller flera användare eftersom lösenordet inte är tillräckligt komplext samt att det inte byts med regelbundenhet.

Idag går det inte att säkerställa att det är rätt person som loggar in i journalsystemet, det finns ingen kontrollfunktion för användaren att granska sina egna loggar i ett förebyggande syfte för intrång där obehörig har loggat in med ens inloggningsuppgifter.

En annan iakttagelse är att användare oftast inte har som vana att låsa datorn när de lämnar skrivbordet, vilket gör att informationen som finns på skärmen blir synlig för andra i två minuter tills datorn låser sig per automatik vid inaktivitet. Vid inaktivitet i mer än 15 minuter blir användaren per automatik utloggad från Cosmic, för att komma in i journalsystemet igen krävs det en ny inloggning.

Verksamhetschefer och enhetschefer har i uppdrag att varje månad genomföra loggkontroll på sina anställda för att säkerställa att användare inte har varit inne och hanterat patientjournaler till patienter de inte har en vårdrelation till. Detta genomförs per automatik i ett system som granskar varje anställd baserad på följande parametrar: familj/anhörig, grannar (går på gatuadress eller fastighetsbeteckning), kollegor (hsa-katalogen), sig själv. Utöver dessa kriterier genomförs även granskning vid misstanke, och då det är kända personer som fått vård på kliniken. Vid eventuell misstanke tar verksamhetschefen/enhetschefen upp fallet med den berörda som i sin tur utreds för intrång, om misstankar föreligger görs en polisanmälan. Det framkommer av intervjuerna att inga ytterligare kontroller genomförs för att fånga upp andra intrång.

Externt intrång

Externa intrång är intrång som sker från en anslutning utanför byggnaden, av en person eller grupp som söker tillgång till information via t.ex. internet eller någon annan åtkomstpunkt. Sätten som angripare använder för att komma åt informationen varierar och förändras med tiden då tekniken utvecklats och nya sårbarheter upptäckts. Utifrån intervjuer framkom det att Region Västmanland arbetar med IT-säkerheten, bl.a. genom att hålla systemen uppgraderade och se till att miljön körs på en modern plattform. De arbetar även med att förenkla inloggningen med SITHS-korten, där en övergång att endast använda kortinloggning skulle innebära en avsevärd höjning av IT-säkerheten. Region Västmanland har även vid flera tillfällen varit föremål för extern granskning som en del av IT-säkerhetsarbetet.

Datum	Företag	Typ av granskning
Februari 2017	PwC	PEN-test och phishing attack
December 2015	PwC	Granskning av landstingets hantering av patientjournal
Juni 2015	PwC	Granskning av fysisk säkerhet av verksamhetskritisk digital information
januari 2015	Atea	PEN-test och phishing attack

2.1.3. Bedömning

Det föreligger kontroll av interna intrång genom den systematiska återkommande kontrollen, dock fångar dessa kontroller inte upp andra former av intrång.

Det kan exempelvis vara:

- när en användare återkommande tittar på en patientjournal där patienten inte fångas upp enligt de kriterierna för den månatliga sökningen
- avvikande beteende fångas inte upp, t.ex. titt i journalen när användaren inte är i tjänst
- skyddade personuppgifter

Inloggningsmetoden med SIHTS-kort uppfyller kraven på stark autentisering i enlighet med 2 kap. 1 § HSLF-FS 2016:40, däremot inte inloggningsmetoden som innehåller endast användarnamn och lösenord. Lösenordsmetoden har brister av två anledningar: avsaknad av komplexitet i lösenordet och att det ej finns krav på att det regelbundet ska bytas. För den enskilde användaren finns det ingen möjlighet att upptäcka om någon annan obehörig har fått tillgång till dennes konto, vilket i praktiken kan göras genom att själv få ta del av samtliga inloggningsloggarna på sitt eget konto.

Arbetet med att hålla IT-säkerheten på en tillfredställande nivå pågår. Ett flertal initiativ såsom att frångå användning av lösenordsmetoden och istället använda SITHS-kort som en ”tvingad” åtgärd är en aktivitet som är uppstartad. Det ska även bli enklare att använda SITHS-kortet än vad det är idag. Återkommande sårbarhetsgranskningar bör göras med tätare intervaller då det ständigt upptäcks nya hot.

Bedömning: Delvis uppfyllt

2.2. Finns process för att kontinuerligt utföra stickprov på behörigheterna i patientjournalsystemet?

2.2.1. Utgångspunkt

PDL betonar vikten av uppföljningskontroller, inte bara för att utreda åtkomst som faktiskt har skett utan även som en preventiv åtgärd. Med en väl fungerande åtkomstkontroll kan ett intrång upptäckas i efterhand och användaren kan tänka sig för innan denne gör något intrång. Det räcker dock inte att bara göra åtkomstkontroller i särskilda fall när ett obehörigt intrång misstänks. Vårdgivaren måste göra systematiska och återkommande kontroller av om det förekommer någon obehörig åtkomst till uppgifter om patienterna.

Vårdgivaren ansvarar även för att det finns rutiner som inkluderar en regelbunden uppföljning av behörigheterna. Genom att regelbundet följa upp behörigheterna kan felaktiga behörigheter, som av någon anledning inte har hanterats i rutinen, fångas upp.

2.2.2. Iakttagelser

Baserad på intervjuerna finns det idag ingen praktisk tillämpbar metod för att genomföra stickprov på behörigheterna i journalsystemet. En rensning har genomförts där regionen har tagit bort personer som inte ska ha tillgång eller en begränsad nivå av behörighet i journalsystemet. I samband med detta upprättades det en användarmanual på hur verksamhetschefen ska gå tillväga vid beställning av behörighet till de anställda.

Regionen arbetar med att utveckla en rapport som ger information om respektive anställds befintliga behörighet. Verksamhetschefen ska använda rapporten som ett verktyg för att kontrollera och säkerställa att behörigheten för respektive anställd är korrekt. Denna är ännu inte framtagen.

2.2.3. Bedömning

Det finns idag ingen process för att kontinuerligt utföra stickprov på behörigheterna i patientjournalsystemet och därmed kan vårdgivaren inte säkerställa att användaren har rätt behörighet.

Bedömning: Ej uppfyllt

2.3. Är den tekniska säkerheten av journalsystemet på en tillfredställande nivå?

2.3.1. Utgångspunkt

För att besvara kontrollfrågan har granskningen fokuserat på nedanstående områden

2.3.2. Iakttagelser

1. Stark autentisering vid inloggning till journalsystemet

Region Västmanland har idag två sätt att logga in till Cosmic. Det är en två-faktor autentisieringslösning som kräver ett fysisk kort och pinkod. Det andra sättet är med namn och lösenord. Lösenordet är något som den anställda fick vid anställning och som det inte finns krav på att byta. Det finns även en del komplexitet med att byta lösenordet då det är integrerat med andra system.

Av intervjuerna har det visat sig att större delen av de anställda har valt att använda användarnamn och lösenord framför SITHS-kort. Den uttalade orsaken att de flesta väljer att inte använda kort är för att Cosmic låses när kortet tas ur datorn och då det är samma kort som används för in- och utpassering så upplevs det som ett ”störelsemoment” i arbetet. Det är något som inte uppstår vid inloggning med namn och lösenord. Region Västmanland arbetar idag med att anpassa lösningen så det ska bli enklare för användarna att använda kort-inloggning.

2. Redundans

För att upprätthålla tillgängligheten till systemet även i situationer där det är stor påfrestning av yttre faktorer så används redundans. Nedan beskrivs Region Västmanlands olika delar av redundans

Redundanta system

Cosmic finns idag i två hallar som båda är aktiva och delar på lasten. Det innebär att vid en händelse av att en hall går ner, så tar den andra hallen över helt utan krav på uppstart eller manuell handpåläggning då den redan är i drift. Systemen mellan hallarna är fullt speglade, och den ena hallen kan när som helst ta över för att kunna arbeta ensam.

Redundanta förbindelser

Region Västmanland har även redundans på dataförbindelserna, där dessa tillhandahålls av två olika leverantörer för ökad tillgänglighet. Med redundans av dubbla dataförbindelser så hanteras t.ex. en incident med att en av fibrerna går ner grävs av, då tar den andra fibern över. I detta fall då det även är redundans med två olika leverantörer så hanteras driftavbrott som uppstår lokalt hos leverantören, då den andra förbindelsen tar över även vid ett sådant driftavbrott.

Redundans på människor

Region Västmanland har ett nära samarbete med sin leverantör Cambio som vid ett problem i Cosmic kan komma in och snabbt hjälpa till att bistå med support. Region Västmanland har även arbetat bort en-personsberoenden till systemet. Även om olika personer är specialiserade på olika delar så har alla i driften åtkomst till Cosmic, och det finns driftdokument på hur Cosmic är uppsatt och med information som behövs vid drift och felsökning.

3. Backup och återställning

För samtliga databaser som Cosmic använder tas både full backup, samt transaktionsloggar. De fulla backuperna körs en gång om dygnet, och transaktionsloggarna backas upp var 15:e minut. Det innebär att vid en stor incident där backuper behövs läsas tillbaka, t.ex. vid ett angrepp av ett ransom virus eller datakorruption, så skulle det i värsta fall vara 15 minuter som man tappar och som behöver registreras om i systemet.
Frontend-servrarna backas upp med snapshots varje dag. Dessa maskiner var enligt intervjuerna lätta att sätta upp på nytt. Så vid en incident så finns möjligheten att ta tillbaka en backup eller sätta upp en ny.

Vid stickprov som utfördes den 21 maj 2018 så har både databas och frontend-servrarna backats upp utan anmärkning de senaste två veckorna.

Återläsning av backuperna sker regelbundet. Dels som tester men även som skarpa återläsningar när det krävs.

4. Uppdatering av systemet

För att upprätthålla en stabil och säker miljö, så krävs det att plattformen fortfarande har support samt att det underhålls med regelbundna säkerhetsuppdateringar.

Det är en modern plattform som systemet körs på och stickprov utfördes (21 maj 2018) för att undersöka om plattformen uppdaterades regelbundet. Vid dessa kontroller framgick det att det sker uppdateringar varje månad. På servrarna som databaserna körs på, var det något längre tid mellan uppdateringarna, men det skedde kontinuerligt och utan anmärkningar.

5. Spårbarhet

Vid en incident, oavsett om det är ett intrång eller uppstått av annan orsak så behövs det tillförlitliga loggar för att i efterhand kunna se vad som hänt i systemet. För att säkerställa att loggarna är tillförlitliga så bör dessa minst innehålla följande information enligt 4 kap. 9 § HSLF-FS 2016:40

Kontroll av detta utfördes 2018-05-21 10:24-10:30

Funktion	Kommentar
Det av dokumentationen av åtkomsten (loggar) framgår vilka åtgärder som har vidtagits med uppgifter om en patient	Systemet loggar en händelse, men under testerna så framgick det inte i loggarna om personen tittade på en anteckning, eller upprättade en. Båda handlingarna flaggas som “getjournalrecordsforsoc”
Det av loggarna framgår vid vilken vårdenhet	Ja
Vilken tidpunkt åtgärderna har vidtagits,	Ja
Användarens och patientens identitet framgår av loggarna	Ja
Systematiska och återkommande stickprovskontroller av loggarna görs	Månatliga automatiserade kontroller görs, men idag utförs inga stickkontroller. Specifika kontroller utförs vid nödöppning av journal, vid särskild händelse eller misstanke.
Genomförda kontroller av loggarna dokumenteras	Ja. Loggranskningen dokumenteras på blanketten Loggranskning journalsystem.
Loggarna sparas i minst fem år	Ja. Det finns ingen gallring uppsatt. Loggarna sparas för alltid.

2.3.3. Bedömning

Region Västmanland har en robust driftmiljö som är väl anpassad att stå emot driftavbrott. IT-miljön som Cosmic körs på är modern och uppdateras kontinuerligt, vilket minskar risken för sårbarheter. Vid en allvarlig incident finns backuper för återställning av databaserna med max 15 minuter dataförlust, från tidpunkten när incidenten uppstod. Det är en brist att det finns möjlighet att logga in med användarnamn och lösenord, framför allt då lösenorden är svaga. Processen för att utföra stickprov i loggarna är borttagna, det bör ses över för att ske regelbundet.

Bedömning: Delvis uppfyllt

2.4. Finns erforderliga processer på plats för att säkerställa behörigheterna i patientjournalsystemet?

2.4.1. Utgångspunkt

I enlighet med HSLF-FS 2016:40 ska vårdgivaren ansvara för att det finns rutiner för att ändra, ta bort och regelbundet följa upp behörigheterna. Behörigheterna ska alltid vara uppdaterade så att dessa är riktiga oavsett om personal börjar, slutar eller får ändrade arbetsuppgifter. Om en användare får nya arbetsuppgifter ska också behörigheten spegla användarens roll.

Behörigheterna ska begränsas till vad som behövs för att den enskilde ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården i enlighet med 4 kap. 2 § PDL.

2.4.2. Iakttagelser

Baserad på intervjuerna finns det idag ingen process eller rutin som säkerställer att varje användare i patientjournalsystemet har rätt behörighet. Det finns idag ett antal grundbehörighet som utgår från användarens yrkesroll med hjälp av HSA-katalog[1] som används när en verksamhetschef ska göra beställning i enlighet med riktlinje 34761-15 “Beställning av Cosmicbehörigheter i HSA- Användarmanual". Utöver grundbehörigheterna finns det ett antal extra behörigheter. Behörigheterna ska vara individuella för att i största mån begränsa åtkomsten i patientjournalsystemet så att rätt användare med rätt åtkomst har tillgång.

Dokumentet “Beställning av Cosmicbehörigheter i HSA- Användarmanual” ger information till beställare om vilka behörigheter som finns för respektive yrkeskategori inklusive extra tillbehörighet för yrkeskategorier med specialistinriktning. Rutinen i sig beaktar inte hur beställaren säkerställer att användaren har rätt behörighet förutom vid nyanställning där användaren inte har någon behörighet inlagd i systemet. Det föreligger inte någon form av kontroll från systemförvaltningens sida att extrabehörigheterna är rimliga när en beställning initierats av en verksamhetschef. Detta innebär att om en användare byter tjänst/roll inom Region Västmanland finns det ingen möjlighet att fånga upp och säkerställa att behörigheterna är korrekt, användaren kan ha en högre behörighet än vad den nya rollen kräver.

2.4.3. Bedömning

I dagsläget finns det ingen process som säkerställer att respektive användare har rätt behörighet i Cosmic. Vid anställning finns det rutiner som säkerställer att en anställd får rätt behörigheter för sin roll, men när en anställd byter tjänst eller verksamhet inom regionen

[1] Katalogtjänst HSA är en elektronisk katalog som innehåller kvalitetsgranskade uppgifter om personer och verksamheter inom svensk vård och omsorg

finns det ingen process som fångar upp om personen har rätt behörigheter. Ett verktyg håller på att arbetas fram av regionen som gör det möjligt att exportera behörighetslista från systemet som förenklar kontroll av korrekt åtkomst/behörighet.

Bedömning: Ej uppfyllt

2.5. Finns det specifika loggar och en process för att analysera dessa?

2.5.1. Utgångspunkt

Vårdgivaren ska ta fram rutiner och processer för ändring, borttagning och regelbunden uppföljning av behörigheterna för att säkerställa att dessa är riktiga och aktuella i enlighet med 4 kap. 3 § HSLF-FS 2016:40.

2.5.2. Iakttagelser

Loggning av all aktivitet som sker i Cosmic lagras i en loggserver som hanteras av Cosmic. Delar av informationen överförs sedan till LoggKoll som är ett egenutvecklat system av Region Västmanland. Samtliga verksamhetschefer, samt personer som har rollen loggranskare och två förvaltningsledare (administratörer på central nivå) har tillgång till systemet.

En gång i månaden ska verksamhetschefen eller loggranskare initiera loggkontroll på sina anställda i syfte för att granska om användare har varit inne i journaler såsom; i sin egen journal, sina anhöriga, kollegor, grannarna eller lokala kändisar. Baserad på våra iakttagelser sker loggkontrollen inte varje månad på samtliga kliniker därför genomförs det en manuell kontroll på centralnivå en gång per år för att säkerställa att samtliga har genomfört den månatliga loggkontrollen.

Utöver den månatliga loggkontrollen med givna granskningsparametrar görs inga andra stickprovsgranskningar.

2.5.3. Bedömningar

Specifika loggar avseende patientjournal samlas i Cosmic där delar av informationen överförs vidare till LoggKoll. LoggKoll möjliggör vidare analys av loggarna för verksamheterna och patienten själv genom 1177.se. Det finns en rutin för hur loggranskningen ska ske för verksamheterna som återfinns i riktlinje för loggranskning 24447-3.

Bedömning: Uppfyllt

2.6. Finns det ett tydligt ansvar för loggarna och kontroll av dessa?

2.6.1. Utgångspunkt

Enligt 4 kap. 9 § HSLF-FS 2016:40 ska vårdgivaren ansvara för loggarna som finns i journalsystemet, visa på spårbarhet (läst, ändrat, skrivit ut, upprättat, identitet på användaren och patienten) samt att det genomförs regelbundna kontroller som dokumenteras.

2.6.2. Iakttagelser

Loggar från patientjournalsystemet finns idag i två system; Cosmic och i LoggKoll (regionens eget utvecklat system). Det finns två förvaltningsledare centralt som ansvarar för att informationen från Cosmic överförs korrekt till LoggKoll varje natt. Verksamhetschefer eller loggranskarna ansvarar för att genomföra den systematiska och återkommande kontrollen samt följa upp loggarna vid behov i enlighet med riktlinjen för loggranskning 24447-3. Tidigare har kontrollen genomförts manuellt genom stickprovsgranskning där samtliga anställda ska gås igenom årligen, detta har nu ersätts fullt ut med den automatiserade kontrollen. Detta innebär att det finns ett antal andra parametrar som inte fångas upp i denna process.

Loggränssnittet i Cosmic används uteslutande vid en inrapporterad händelse eller incident, utöver det används det inte.

2.6.3. Bedömning

Det finns en tydlig ansvarsfördelning avseende loggarna på både central- och på verksamhetsnivå som uppfyller kraven i enlighet med 4 kap. 9 § HSLF-FS 2016:40. Återkommande kontroller av loggarna sker månatligen där verksamhetschefen/loggranskarna är ansvariga för att det genomförs.

Bedömning: Uppfyllt

3. Bedömningar mot kontrollmål

Kontrollmål	Kommentar
Finns det kontroller avseende intrång?	**Delvis uppfyllt** Det finns kontroller för att upptäcka intrång. Inloggningen i Cosmic kan ske på två sätt varav den ena inte uppfyller kraven på stark autentisering
Finns process för att kontinuerligt utföra stickprov på behörigheterna i patientjournalsystemet?	**Ej uppfyllt** Ingen process för att kontinuerligt utföra stickprov på behörigheterna i patientjournalsystemet och därmed kan vårdgivaren inte säkerställa att användaren har rätt behörighet
Är den tekniska säkerheten av journalsystemet på en tillfredställande nivå?	**Delvis uppfyllt** Det arbetas med säkerhet, och det finns delar som visar på god säkerhet dock finns det brister med inloggningen till Cosmic.
Finns erforderliga processer på plats för att säkerställa behörigheterna i patientjournalsystemet?	**Ej uppfyllt** Finns ingen process som säkerställer att användare har rätt behörighet i Cosmic.
Finns det specifika loggar och en process för att analysera dessa?	**Uppfyllt** Loggarna för journalsystemet finns både i Cosmic och i LoggKoll. Analys av loggarna sker vanligtvis direkt från LoggKoll av verksamhetschefen eller utsedda loggranskare
Finns det ett tydligt ansvar för loggarna och kontroll av dessa?	**Uppfyllt** Det finns en tydlig ansvarsfördelning avseende loggarna på både centralnivå och på verksamhetsnivå. Återkommande kontroller av loggarna sker månatligen

3.1. Sammanfattande revisionell bedömning

Vi bedömer att regionstyrelsen för Region Västmanland delvis har en god säkerhet i patientsystemet och hantering av patientjournaler, men vi har uppmärksammat ett antal brister som måste ses över.

Vi grundar vår bedömning på den avstämning av kontrollmål som gjorts genom intervjuer och stickprovsgranskning. Regionen har en robust IT-miljö för att hantera avbrott och driftstopp dock finns det en viss avsaknad av processer och rutiner för att kontrollera essentiella uppgifter såsom rätt behörighet eller att det är rätt användare som loggar in i Cosmic med användarnamn och lösenord. Det framkom under intervjuerna att regionen delvis är medvetna om bristerna och arbetar med att se över det. Till hösten ska regionen implementera att inloggning i Cosmic endast sker med SITHS-kort, vilket medför en betydligt säkrare inloggning än det som tillämpas idag med lösenordsmetoden. Den månatliga loggkontrollen uppfyller kraven för att genomföra regelbundna systematiska kontroller av loggarna dock kan det missas av verksamheterna att genomföra detta varje månad, vilket enbart fångas upp en gång per år i form av en manuell kontroll av systemförvaltaren.

Bilaga 1

Intervjuade personer under perioden april-maj 2018

Roll
Läkare, användare av Cosmic
IT-chef, systemägare teknik
Systemägare verksamhet
Enhetschef, superuser
Läkare, tidigare superuser, idag användare
Enhetschef
Informationssäkerhetskoordinator
Systemförvaltare
Systemförvaltare
Systemförvaltare
Driftansvarig
Administratör logghantering

Bilaga 2

Granskade dokument

Dokument	Namn	Beslutat datum	Ägare till dokument går att utläsa	Version	Kommentar
Riktlinje för sekretess och tystnadsplikt	2569 Sekretess och tystnadsplikt i Region Västmanland - Riktlinje.doc	2017-08-29	Ja	2569-3	
Riktlinje för åtkomst till patientuppgifter i journal	19747 Åtkomst till patientuppgifter i journal - Riktlinje.doc	2018-01-15	Ja	19747-3	
Riktlinje för loggranskning	24447 Loggranskning - Riktlinje.doc	2017-03-28	Ja	24447-3	
Riktlinje för rät att ta del av journaluppgifter vid sammanhållen journalföring	28979 Rätt att ta del av journaluppgifter vid sammanhållen journalföring - Riktlinje.doc	2016-02-02	Ja	28979-1	
Instruktion för besällning av behörigheter	34761 Beställning av behörigheter Cosmic.docx	2018-03-02	Ja	34761-15	
Instruktion för backup och återställning	SQLRES_Disaster_Recovery_Plan_LTV.docx	Ej beslutat. Utfärdat 2014-07-10	Nej		HP har tagit fram instruktioner för backuphantering. Detta är en mall, men har ej blivit implementerad i organisationen.
Driftdokumentation/ Beredskapsinformation	Cosmic-Drift_beredskapsinfo2012.doc		Ja	0.6	

2018-06-04

Uppdragsledare
Tobias Bjöörn

Projektledare
Mikael Grönvik