Vännäs kommun

Behörigheter och loggkontroll

Revisionsrapport

KPMG AB
2015-12-14
Antal sidor: 13

Innehåll

1. Sammanfattning med kommentarer

Vi har av revisorerna i Vännäs kommun haft i uppdrag att granska hanteringen av behörigheter och åtkomstkontroll i kommunens datoriserade verksamhetsstöd avgränsat till Magna Cura HSL och LSS vid vård- och omsorgsförvaltningen. Behörighetsstyrning och åtkomstkontroll är en viktig och central komponent i kommunens arbete med informationssäkerheten.

Vi har granskat styrdokument, intervjuat samt analyserat data från Magna Cura (användarinformation och loggar), anställningsdata från PA-systemet samt utdrag ur kommunens katalogsystem (AD: et). Granskningen har varit inriktad mot att avgöra om tilldelningen av behörigheter följer de styrande dokumenten och via analysen göra bedömningar hur man lyckas efterleva dem i praktiken. Hur kontroll av loggad information utförs har här särskilt analyserats.

Från granskningen vill vi särskilt framhålla följande:

Styrande dokument av tillämpningskaraktär för informationssäkerhet från kommunövergripande till verksamhetsspecifika lyser med sin frånvaro. Det finns en äldre informationssäkerhetspolicy antagen av KF. För att kommunens olika verksamheter ska ha en övergripande kunskap och kännedom om vad som gäller i kommunen avseende informationssäkerhet är det väsentligt att ansvariga skyndsamt påbörjar ett arbete med att utarbeta en ny eller uppdatera innevarande policydokument. Det är högst väsentligt att detta dokument kompletteras med tydliga och praktiska tillämpningsföreskrifter inte minst vad gäller behörighetshantering. Vad gäller tillämpningsföreskrifter så utarbetas och antas riktlinjerna (vad göra i förhållande till de mål som framgår av policydokumentet) med fördel i den sammanslutning av tjänstemän som bildar kommunens ledningsgrupp. Anvisningar och instruktioner (vem, när, var och hur) baserade på den kommunövergripande riktlinjen beslutas med fördel på lämpliga nivåer i linjeorganisationen. Allt för att uppnå integration och god anpassning till de informationsrisker som via risk- och väsentlighetsanalyser identifieras i respektive verksamhet. Med andra ord styrningen för det som granskats i detta uppdrag är svag till obefintlig. (8.1 och 8.2)

Logg i Magna Cura har *aldrig kontrollerats* vare sig under granskningsperioden eller sedan systemet sattes i drift 2014. Systematisk loggkontroll[1] görs för att den enskilde ska känna sig trygg med att ingen obehörig personal tar del av information som denne inte är behörig till. Vårdgivare av hälso- och sjukvård är skyldig att kontrollera att inga obehöriga tar del av patientuppgifter och att personal inte tar del av information som de inte behöver ha tillgång till för att utföra sitt arbete. Den som bedriver verksamhet inom socialtjänst är skyldig att tillse att inga obehöriga tar del av information som de inte behöver ha tillgång till för att utföra sitt arbete. Vi anser att ändamålsenliga och effektiva instruktioner och metoder utan fördröjning upprättas, formellt beslutas och införs (8.3)

Vid granskningstillfället kunde noteras att möjligheten att radera/utplåna delar av journaler använts. Det är väsentligt att kunna redogöra för hur detta har varit möjligt samt att upprätta styrande dokument om hur detta, om det finns motiv, i framtiden ska hanteras. Behörighet att hantera utplåning ska begränsas till verksamhetsansvariga. (8.3 och 8.5)

[1] 4 kap. 3§ patientdatalagen och 2 kap. 11§ SOSFS 2008:14. Bestämmelserna kompletterar bestämmelsen om inre sekretess i 4 kap. 1§ patientdatalagen.

Det saknas en formaliserad och dokumenterad tilldelning av behörigheter. Användningen, ordningen, fullständigheten och riktigheten i det urval vi granskat, 22 identiteter, gör att vi rekommenderar en genomgång av alla tilldelade behörigheter för att identifiera om det finns ytterligare brister än de vi noterat. Vi noterar att det saknas underlag för majoriteten beställningarna. Personer har dubbla identiteter och några finns inte i anställningsregister och/eller i den centrala katalogtjänsten (AD:et). Alla identifierade brister inklusive de administrativa förändringar som identifieras bli nödvändiga måste åtgärdas för att det ska vara möjligt att göra bedömningen att behörighetshanteringen är säker och ändamålsenlig. (8.4)

Vi redovisar ett större antal rekommendationer baserat på vår analys av loggdata från Magna Cura. Vi anser att dessa både kan och ska användas som urvalsunderlag när loggkontroller utförs. Enstaka exempel motiverar kanske inte ett urval. En kombination av rekommendationer som omfattar samma person gör dock rimligtvis hen betydligt mer aktuell för en kontroll. (8.3 och 8.5)

2. Bakgrund

Vi har av revisorerna i Vännäs kommun haft i uppdrag att granska hanteringen av behörigheter och åtkomstkontroll i kommunens datoriserade verksamhetsstöd avgränsat till Magna Cura HSL och LSS vid vård- och omsorgsförvaltningen.

Verksamheternas utveckling i en kommun har med åren blivit alltmer IT-beroende vilket innebär nya former av hot och risker. Behörighetsstyrning och loggkontroll blir då i sammanhanget en viktig och central komponent i kommunens arbete med informationssäkerheten. Detta arbete innebär bland annat upprättande och upprätthållande av rättigheter för användare så att dessa enbart får och har åtkomst till den information som de behöver i sitt dagliga arbete.

3. Syfte

Syftet med granskningen har varit att besvara följande frågekomplex:

- Vilka styrdokument (policy med tillhörande riktlinjer, anvisningar och instruktioner) finns som kommunövergripande hanterar behörighetstilldelning? Finns det verksamhetsspecifika dokument som ställer ytterligare och mer detaljerade krav för det system granskningen avgränsats till?

- Finns det särskilda anvisningar och instruktioner för:

  - Personer som *inte* är tillsvidareanställda eller uppdragstagare?

  - Systemleverantörer, implementeringskonsulter, extern supportpersonal etc?

- Hur säkerställs kunskapen om och efterlevnaden av styrdokumenten i den verksamhet som granskningen avgränsats till?

- I vilken omfattning, när, hur och efter vilka anvisningar utförs så kallade loggkontroller?

- I vilken omfattning och på vilket sätt berörs behörighetshantering och loggkontroller i internkontrollplanerna?

- På vilken analysgrund, på vems verksamhetsansvar har det dokumenterats och tilldelats behörigheter för personal:

  - Som vid granskningstillfället använder det verksamhetsstöd som granskningen är avgränsad till?

  - Knuten till IT-avdelningen?

- Vad framkommer när vi jämför personförekomst i PA-systemet, med vad som framgår av den centrala katalogtjänsten (AD: et) och data från granskat verksamhetssystem??

4. Avgränsning

Granskningen har varit avgränsad att omfatta det verksamhetssystem som används inom vård och omsorgsförvaltningen (Magna Cura HSL och LSS). Granskning omfattar inte val av autentiseringsmetoder.

5. Revisionskriterier

De kriterier som har legat till grund för bedömning och rekommendationer är hämtade från kommunallagens 6 kapitel samt reglemente för intern kontroll och tillämpningsanvisningar.

Den interna kontrollen är viktig att utgå från då den är ett medel för ledningens kontroll av att verksamheten efterlever lagar, förordningar, policys och riktlinjer. Intern kontroll är en process vilken styrelsen, ledningen och annan personal skaffar sig rimlig säkerhet för att målen uppnås och som påverkas av hur man agerar i vad man säger och utför.

Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården SOSFS 2008:14[2].

6. Ansvarig styrelse

Granskningen avser kommunstyrelsen samt vård- och omsorgsnämnden.

7. Metod

Granskningen har genomförts genom dokumentstudier och initiala intervjuer med systemförvaltare. I en gruppintervju 2016-12-02 där, förutom representanter för revisionen och systemförvaltarna medverkade, medicinskt ansvarig sjuksköterska[3], socialchef, personalchef, IT-chef, IT-tekniker, chef/kvalitetsledare för individ- och familjeomsorgen, områdeschef hälso- och sjukvårdsenheten, personalenhetens chef samt chefer inom LSS-omsorgen. Utöver detta har BKS[4]-data från verksamhetssystem inhämtats för jämförelse med person- och anställningsregister samt vad som framgår av kommunens centrala katalogtjänst (AD[5]: et). Granskningsperiod har varit januari till oktober 2016. Rapporten är ännu inte faktagranskad av systemförvaltarna.

8. Granskningsnoteringar

Noteringarna redovisas avsnittsvis med kommentarer i samma ordning revisionsfrågorna anges under avsnittet syfte ovan.

---

[2] Patientdatalagen (2008:355) och Socialstyrelsens föreskrifter (SOSFS 2008:14) om informationshantering och journalföring i hälso- och sjukvården utgör viktiga led i förverkligandet av den nationella IT-strategin för vård och omsorg.

[3] Medicinskt ansvarig sjuksköterska förkortas vanligtvis MAS

[4] BKS en förkortning av behörighetskontrollsystem.

[5] Active Directory, AD, är en katalogtjänst från Microsoft som innehåller information om olika resurser i en domän (nätverk) till exempel, datorer, skrivare och användare. Dessa klassificeras som objekt och kan hanteras samt skyddas i den egna domänen.

8.1 Vilka styrdokument finns som kommunövergripande hanterar behörighetstilldelning[6]?

I februari 2009 antog kommunfullmäktige (KF) en informationssäkerhetspolicy. Vid samma tidpunkt nämns i protokollet inget om i vilken omfattning och var i organisationen de tre informationssäkerhetsinstruktionerna, som redovisas i policydokumentet, ska upprättas. Enligt uppgift så ska verksamhetsanknutna tillämpningsföreskrifter upprättas inom respektive förvaltning.

Av en blankett som använts vid hantering av behörigheter ”Rutin för behörigheter (Bilaga 7)” beslutad av IT-chef med fastställelsedatum 2013-10-01 ska det på kommunens intranät finnas en avdelning benämnd Informationssäkerhet. När vi och systemadministratörerna 2016-11-30 söker efter dokument om informationssäkerhet på intranätet hittar vi inga förutom informationssäkerhetspolicyn.

Blankettens informationsdel innehåller i övrigt tydliga instruktioner om hur behörigheter övergripande ska hanteras. Av ytterligare en blankett, ”Beställning av användaridentitet(er)” daterad 2006-04-05, som vi iakttar ha använts vid behörighetshantering framgår att: ”Användaridentiteter ska beställas med denna blankett då all behörighetsadministration ska dokumenteras och sparas. Respektive avdelningschef (... ÄO-chef … MAS …) är ansvarig för vilka behörigheter verksamhetens personal ska ha.” Vidare framgår att: ”Därtill har enhetscheferna inom HO och ÄO delegation att beställa användaridentiteter.” Avseende kontroll av behörigheter framgår av 2013 års blankett att ”Respektive systemadministratör kör ut en lista på användare och deras behörigheter varje år i mars månad. Listan lämnas till närmaste chef för kontroll.” Vi har efterfrågat listor hos systemadministratörerna och chefernas noteringar rörande den utförda kontrollen för 2016 och kan konstatera att inga listor har efterfrågats och därför inte producerats. Följaktligen har då inga kontroller utförts.

Ett komplement till policyn benämnd systemsäkerhetsplan[7], aktuell vid den tidpunkt policyn beslutades, finns inte upprättad för det verksamhetssystem som omfattas av denna granskning. Vad gäller behörigheter hänvisar därmed policydokumentet inte till någon tillämpningsföreskrift som anger och specificerar allmänna riktlinjer.[8]

Informationssäkerhetspolicyn, det enda kommunövergripande styrdokumentet som kan iakttas, baserar sig på rekommendationer från en myndighet som inte längre existerar, Krisberedskapsmyndigheten (KBM[9]). Den myndighet som nu hanterar frågor om informationssäkerhet är

[6] Med behörighetstilldelning menas här även förändring och avveckling av behörigheter.

[7] Systemsäkerhetsplan (senare ersatt av systemsäkerhetsanalys): Dokument avseende ett enskilt informationssystem eller internt IT-nätverk som redovisar de samlade kraven på detta avseende tillgänglighet, riktighet och sekretess (konfidentialitet). Av säkerhetsplanen ska framgå vilka säkerhetsåtgärder som är vidtagna samt de eventuella ytterligare säkerhetsåtgärder som behöver vidtas för att kraven på informationssystemet ska uppfyllas. Säkerhetsplanen ska vara avstämd mot informationssäkerhetspolicyn.

[8]En dokumentation som med underlag av en riskanalys anger minimikrav.

[9] KBM inrättades 2002 efter beslut av riksdagen. Samtidigt upphörde Överstyrelsen för civil beredskap (ÖCB). Riksdagen beslutade 20 maj 2008 att en ny myndighet skulle inrättas 1 januari 2009 och att KBM, Statens räddningsverk och Styrelsen för psykologiskt försvar skulle läggas ned. Den nya myndigheten, Myndigheten för samhällsskydd och beredskap (MSB), har en samordnande roll i krisberedskapsarbetet.

Myndigheten för samhällsskydd och beredskap (MSB). De tillsammans med SKL[10] tillhandhåller stöd och råd i informationssäkerhetsfrågor på siten www.informationssäkerhet.se

Kommunens övergripande styrning av informationssäkerheten baserar sig på äldre rekommendationer och på stöd samt hjälpmedel som inte längre underhålls. I nedanstående avsnitt redovisar vi effekten av detta.

Vi har efter intervjuer anledning att förmoda att det även saknas tillämpningsföreskrifter för övriga informationssäkerhetsområden som berör granskad verksamhet. Detta trots att protokollet från KF: s sammanträde 2009-02-23 avslutas med ett beslut lydande: ”Informationssäkerhetspolicy för Vännäs kommun antas och skall gälla samtliga förvaltningar. Information och uppföljning skall ske årligen till kommunstyrelsen.” Ansvarig för detta anges vara kommunchefen som ”har det övergripande ansvaret för informationssäkerheten och utser systemägare för respektive informationssystem.” Av denna rollfördelning framgår även att systemförvaltarna ”utses av respektive systemägare och ansvarar för den dagliga användningen av informationssystemen.”

Kommentar

Ansvariga ska inte tveka att så fort tillfälle ges starta ett arbete med att revidera, uppdatera modernisera och komplettera det för dagen gällande dokumentet till en policy som möter moderna verksamheters krav. Alternativt så inför man i tillämplig omfattning ett ledningssystem för informationssäkerhet (LIS[11]). Görs ett sådant val är det fullt möjligt att återanvända befintlig styrdokumentation likaväl som beskrivningar på blanketter förutsatt att den är aktuell och korrekt. Vad vi kan bedöma är det inte endast informationssäkerheten fokuserad på behörigheter som behöver en uppdatering utan hela arbetet med att integrera, prioritera, informera och utbilda i informationssäkerhet i all den verksamhet kommunen bedriver. Uppdaterat, alternativt nytt, policydokument antas i KF. Vad gäller tillämpningsföreskrifterna tas riktlinjerna (vad göra i förhållande till de mål som framgår av policydokumentet) med fördel i den sammanslutning av tjänstemän som bildar kommunens ledningsgrupp. Anvisningar och instruktioner (vem, när, var och hur) baserade på riktlinjen beslutas med fördel på lämpliga nivåer i linjeorganisationen. Allt för att uppnå integration och god anpassning till de informationsrisker som identifieras i respektive verksamhet.

8.2 Särskilda anvisningar för behörighetstilldelning

Vård- och omsorgsförvaltningen har inte infört några särskilda och formellt antagna tillämpningsföreskrifter för hanteringen av informationssäkerheten i det verksamhetssystem som omfattas av granskningen. KBM: s och senare MSB: s stöd för bedömning och hantering av informationssäkerheten, BITS[12], uppges ha använts för det verksamhetssystem som användes innan innevarande system. BITS som stöd utvecklas och stöds inte längre av MSB utan det hänvisas till att använda ett LIS. Det uppges finnas ett embryo till tillämpningsföreskrifter omfattande det område som

[10] Sveriges Kommuner och Landsting

[11] LIS ett modernt metodstöd som riktar sig till de som ska bedriva informationssäkerhetsarbete t ex i en kommun. Stödet utgår fram för allt från standarderna i ISO 27000-serien. Läs mer på www.informationssäkerhet.se.

[12] Basnivå för informationssäkerhet.

granskas. När och i vilken omfattning dessa kommer att formellt antas och införas är vid granskningstillfället inte känt.

Kommentar

Det saknas väsentliga och tydliga instruktioner för behörighetstilldelning. På vård- och omsorgsförvaltningen måste det finnas en väl känd dokumentation med tydligt beskrivna anvisningar och instruktioner vars efterlevnad ska säkerställs. Rimligen så upprättas snarast sådana vilka harmonierar med, och där det bedöms nödvändigt förstärker, de kommungemensamma tillämpningsföreskrifterna. Vi bedömer det högst väsentligt att detta arbete prioriteras.

Detta understryker även vår tidigare kommentar att det inte är orimligt att anta att en analys av informationssäkerhetsläget i kommunen som helhet kommer att resultera i att informationssäkerhetsarbetet och de befintliga styrdokumenten uppdateras.

8.3 Kontroll av loggar och internkontroll

8.3.1 Kontroller

Av våra intervjuer framgår att det aldrig utförts någon kontroll av loggar[13] under granskningsperioden. Kontroll har vad vi förstår inte utförts någon gång sedan systemet infördes 2014. Det finns inga instruktioner och rutiner dokumenterade och etablerade för hur detta ska gå till. SOSFS 2008:14 är tydlig med att detta ska finnas. Logghantering i Magna Cura har heller inte varit ett internkontrollmål i den internkontrollplan som var aktuell inom granskningsperioden.

8.3.2 Utplåning av journalanteckningar

Vi vet av erfarenhet att det går att tilldela behörigheter till roller som kan innebära möjlighet att utplåna[14] journalanteckningar. Vår analys av loggen, vilken redovisas i avsnitt nedan, indikerar att en inte obetydlig mängd användare har utnyttjat en funktion i Magna Cura som innebär att patientdata kan ha utplånats. Vi har i samband med granskningen för systemadministratörerna presenterat en sammanställning på användare som är loggade för händelsen ”radera”. Den visar inom vilka delar av systemet (så kallade bilder) som händelsen använts och vi har bett om en och fick en muntlig redovisning 2016-11-30 om vad som raderats. Redovisningen visar att det finns användare

[13] Vårdgivaren måste enligt 4 kap. 3 § patientdatalagen (2008:355) göra åtkomstkontroller för att säkerställa att personalen inte använder sina behörigheter på fel sätt genom att läsa, ändra eller ta bort information som de inte ska hantera. Exempel på en felaktig åtkomst kan vara att någon tittar i en patientjournal trots att han eller hon inte deltar i vården av den patienten. Ett olovligt intrång och olovligt efterforskande i elektroniska informationssystem, till exempel ett journalsystem, kan vara straffbart enligt straffbestämmelsen om dataintrång. Den som ”olovligen bereder sig tillgång till upptagning för automatisk databehandling eller olovligen ändrar, utplånar, blockerar eller i register för in en sådan uppgift” döms enligt 4 kap. 9 c § brottsbalken för dataintrång till böter eller fängelse i högst två år. Bestämmelsen torde vara tillämplig om någon använder sin behörighet till ett elektroniskt journalsystem för att läsa uppgifter om en patient utan att informationen behövs, till exempel på grund av nyfikenhet. Enligt rättspraxis kan även läsning i utbildningssyfte räknas som dataintrång, även om användaren söker förebilder på lämpliga formuleringar (RH 2002:36).

[14] Rutinerna för hantering av patientuppgifter ska även säkerställa att uppgifter i patientjournalen inte kan ändras eller utplånas (låsas) annat än med stöd av bestämmelserna i patientdatalagen (2008:355). Rutinerna ska vidare säkerställa att uppgifterna låses en viss tid efter det att de har förts in i patientjournalen, dock senast efter fjorton dagar.

som utplånat data som bedöms vara journalanteckningar. Utplåning har gjorts av fler än en användare rörande fler än en vårdtagare. Vad vi förstår har utplåningen skett utan dokumenterat stöd enligt bestämmelserna i patientdatalagen. Verksamhetsansvariga har inte framställt och formellt beslutat om dokumenterade rutiner som instruerar vem, hur, under vilka förhållande och med vilken dokumentation och kommunikation detta får ske.

8.3.3 IT-kontoret

Enligt uppgift så utför inte IT-kontoret några former av loggkontroller i Magna Cura: s databas. Anledningen till det uppges vara att några sådana uppdrag inte erhållits från systemägaren.

Kommentar

Systematisk loggkontroll[15] görs för att den enskilde ska känna sig trygg med att ingen obehörig personal tar del av information som denne inte är behörig till. Vårdgivare av hälso- och sjukvård är skyldig att kontrollera att inga obehöriga tar del av patientuppgifter och att personal inte tar del av information som de inte behöver ha tillgång till för att utföra sitt arbete. Den som bedriver verksamhet inom socialtjänst är skyldig att tillse att inga obehöriga tar del av information som de inte behöver ha tillgång till för att utföra sitt arbete.

Vi anser att instruktioner och metoder som ska användas ska vara ändamålsenliga och effektiva för att upptäcka och förhindra att journaluppgifter eventuellt hanteras av obehöriga. Avsaknaden exemplifieras nedan med några rekommendationer till nödvändig upprustning. Fler rekommendationer återfinns i skrifter från Socialstyrelsen:

- Alla, externa likaväl som interna (anställda/uppdragstagare) som använder systemet över en given tidsperiod ska omfattas av kontroll.
- Urvalmetodiken är sådan att analyserbara indikationer används så att riskbeteenden ligger till grund för urvalet.
- Om stickprov och slump ska användas som urvalsmetod ska den vara statistiskt säkerställd och representativ för populationen av loggade personer. Hänsyn ska även tas till beslutade kontrollmål.
- Beakta även vad Datainspektionen skriver på sin hemsida. ”Bestäm med vilken omfattning (antal och tidsintervall) loggguppföljningen ska ske. Eftersom det inte enbart är antalet loggposter vid loggguppföljningen som avgör om kontrollen blir verkningsfull, finns det inget generellt svar på hur många loggposter som bör granskas vid varje tillfälle. Varje vårdgivare måste ta hänsyn till verksamhetens omfattning (antalet patienter och personal med behörighet) samt vilket urval och vilken systematik som används vid uppföljningen.”
- Bedömning över tid av loggdata ska göras på samma sätt och på samma grunder oavsett vem som utför den. Här ska det även ingå hur en kontroll kan överlämnas för överprövning.

[15] 4 kap. 3§ patientdatalagen och 2 kap. 11§ SOSFS 2008:14. Bestämmelserna kompletterar bestämmelsen om inre sekretess i 4 kap. 1§ patientdatalagen.

- Det ska utföras en genomgång av loggdata med berörd personal så att eventuella oklarheter eller osäkerheter som framgår av loggdata får sin förklaring.

- Resulterar kontrollen i åtgärder så ska detta leda till att vederbörandes personalakt uppdateras med information om vilka åtgärder som vidtagits.

- Alla användare ska omfattas av loggkontroll, även chefer och verksamhetsextern personal samt personal som har tillgång till journaldata utanför det ordinarie användargränssnittet.

- Hanteringen av dokumentationen från loggkontrollen ska vara enhetlig och hanteras på ett sätt så att informationen som uppdaterar personalakter beaktar vad som framgår av personuppgiftslagen och från och med maj 2018 dataskyddsförordningen.

- Dokumentationen av loggkontroller är allmän handling, därför måste den sparas på ett sätt så att den är hålls fullständig och oförändrad. Det ska även vara enkelt att identifiera och återfinna enskilda dokument. Detta innebär *inte* att förvaringen av dokumenten omedelbart ska vara tillgänglig för alla. Verksamhetsansvariga måste över tid kunna säkerställa att syftet med att få ta del av dokumentation överensstämmer med vad som lämnas ut.

- Av SOSFS 2008:14. framgår att loggkontroller ska sparas i 10 år. Det måste finnas processer/rutiner som säkerställer att så sker och att informationen under denna tid inte kan förändras eller förstöras.

- Av all dokumentation ska framgå vem/vilka som upprättat respektive beslutat, när det skett samt tidsomfattningen av loggdata.

Vi rekommenderar att det i samband med yttrandet över denna rapport lämnas en skriftlig redogörelse om anledning till och omfattningen av vad verksamhetsansvariga anser vara journaldata som utplånats under granskningsperioden. Verksamhetsansvariga ska inte tveka att snarast upprätta styrande dokument som beskriver vad som krävs när det anses finnas och kan anges motiv för utplåning av journalanteckningar. Vi anser att det snarast möjligt sker en översyn av roller och behörigheter i Magna Cura så att det inte föreligger risk för att journalanteckningar oavsiktligt utplånas och/eller förvanskas (händelsen ”Radera” i Magna Cura) med konsekvensen att journaler får ett ofullständigt och därmed missvisande innehåll. Behörighet att utplåna ska endast ges till verksamhetsansvariga så att raderingen/utplåningen endast sker enligt formellt beslutade styrande dokument.

I avsnittet nedan redovisar vi ett antal iakttagelser gjorda vid genomgången av 1 061 282 loggrader omfattande granskningsperioden. Vi rekommenderar att även dessa iakttagelser beaktas när instruktioner övervägs och utformas.

För att loggen i sin helhet ska vara tillgänglig under 10 år så måste det säkerställas att det löpande finns en säkerhetskopia som fullständigt och riktigt omfattar loggen. Det är systemägarens ansvar att så sker genom att detta förfaringssätt beställs av över tid ansvarig för driften av systemet. Eftersom en sådan beställning (del av en systemsäkerhetsplan eller en aktivitet i ett LIS) inte finns vid granskningstillfället ska den snarast upprättas. I den beställningen är det högst lämpligt att det kompletteras med instruktioner om hur den ska förvaras (Konfidentialitet) och att det säkerställs att den över tid är återläsningsbar (Tillgänglighet).

8.4 På vems verksamhetsansvar tilldelas behörigheter?

För att få behörighet[16] till Magna Cura krävs inte alltid en administrativ åtgärd som dokumenteras på en blankett som sparas för kontroll och underlag vid förändringar. I vårt urval av användar-identiteter som vi använt för att undersöka hur och vem de fått sin behörigheter noterar vi att olika blanketter använts. E-post och telefonsamtal samt kommunens ärendehanteringssystem har också använts i kommunikationen med systemadministratörerna. I flera fall kan ingen dokumentation uppvisas om vem som beställt vilken behörighet för användaren.

Vad vi förstår har inte IT-kontorets personal eller personal från annan förvaltning tillgång till Magna Cura via det ordinarie användargränssnittet. Av intervjuerna framgår att det inte finns något sekretessavtal med externa konsulter.

Genom att med underlag av våra analyser välja ut 22 användare och/eller användaridentiteter (”Sign” i Magna Cura) och be om ett analys-/besluts-/beställningsunderlaget iakttar vi följande:

- En blankett har använts för tre användare, e-post från systemägaren för två och telefonsamtal från biträdande socialchefen för en.
- Någon form av underlag saknas för 16 användare.
- Det finns flera användare som innehar och/eller innehaft fler än en användaridentitet. En av dessa återfinns i loggen med en testidentitet.
- Det är programleverantören som själv lagt upp sin egen användaridentitet. Hur många enskilda konsulter som kan använda/har använt den är inte känt och det finns ingen dokumentation innehållande förbehåll hur identiteten ska och får användas.
- Tio av dem där underlag för behörighet saknas återfinns i loggen för att de tagit del och/eller skapat journalanteckningar.
- Fyra av dem där underlag saknas återfinns inte i loggen vilket rimligtvis innebär att de under granskningsperioden *inte* tagit del av förstahandsuppgifter om vårdtagare.
- Fem av dem där underlag för behörighet saknas återfinns i loggen med händelsen ”Radera”. Vilket gör att de omfattas av den undersökning som vi i ovan avsnitt rekommenderar utförs för att klarlägga om detta innebär att de på oriktiga grunder utplånat journalanteckningar.

Kommentar

Det är otillfredsställande, och en tydlig avvikelse i förhållande till vad som framgår av SOSFS 2008:14, att det inte finns en tydlig, efterlevd, formaliserad och dokumenterad hantering av behörigheter. Användningen, ordningen, fullständigheten och riktigheten i det urval vi granskat gör

[16] I 2 kap. 6 § SOSFS 2008:14 anges att vårdgivaren ska ansvara för att det i ledningssystemet finns rutiner som säkerställer att hälso- och sjukvårdspersonalens och andra befattningshavares behörighet begränsas till vad som är nödvändigt för att ge en god och säker vård. Vårdgivaren ska vidare ansvara för att varje användare tilldelas en individuell behörighet för åtkomst till patientuppgifter. Vårdgivarens beslut om tilldelning av behörighet ska föregås av en behovs- och riskanalys. Vårdgivaren ska även ansvara för att det finns rutiner för tilldelning, förändring, borttagning och regelbunden uppföljning av behörigheterna.

att vi rekommenderar en genomgång av *alla* tilldelade behörigheter för att se om det finns ytterligare brister än de vi noterat. Alla identifierade brister inklusive de administrativa förändringar som identifieras bli nödvändiga måste åtgärdas för att det ska vara möjligt att göra bedömningen att behörighetshanteringen i Magna Cura kan bedömas vara säker och ändamålsenlig.

Även så kallade funktionsbehörigheter (om och när sådana används), behörigheter för konsulter och uppdragstagare måste omfattas av en formaliserad hantering där det finns en ansvarig som beställer. Kommunexterna behörigheter bör omgärdas av detaljerade föreskrifter om vad de får utföra inkluderande att de inte får överlåtas till annan utan godkännande från ansvarig beställare. Behörigheterna ska även vara tidsbegränsade. Under längre bortovaro ska de avaktiveras alternativt avvecklas.

För system som Magna Cura är det även utomordentligt viktigt att det finns instruktioner som innebär stor restriktivitet i eventuell tilldelning av databasåtkomst. Det ska klart och tydligt framgå vem som över tid har tillgång till vilka databaser och på vems skriftliga beställning.

8.5 Jämförelse av personförekomst i PA-systemet, i den centrala katalogtjänsten och data från respektive verksamhetssystem.

Vi har jämfört data ifrån de källor som nämns i rubriken. Nedan redovisar vi de iakttagelser inklusive kommentarer vi gjort baserat på:

- 1 061 282 loggrader från Magna Cura.
- Kontodata för 673 användaridentiteter av Magna Cura.
- De 477 användaridentiteter som förekommer i loggen under granskningsperioden. Av de 477 är det 428 stycken som enligt systemleverantörens definition är registrerade för händelser som påverkar vårdtagare.
- 2 088 personers anställningsdata i kommunens PA-system.
- 1 922 identiteter i AD: et.

Beroende på system kan en identitet vara en person eller en funktion. En person kan beroende på system även vara knuten till fler än en identitet. Att det finns färre identiteter i AD än i PA-systemet är en effekt av att anställdas som avslutat sin anställning efter en tid gallras i AD. Iakttagelser och kommentarer redovisas under samma punkt i avsnitten nedan.

Från jämförelser med bäring på användare av Magna Cura noterar vi följande:

- Vi identifierar personer i PA-systemet som med ledning av befattningstexter (legitimerad, men även viss omvårdnadspersonal) borde ha en identitet registrerad i Magna Cura under granskningsperioden men inte har det. Förhållandet innebär risk för att dessa personer inte tar del av information som de ska. Alternativt använder de någon annans identitet, uppdaterar inte systemet eller låter någon annan göra det. Därmed kan inte uteslutas att personer gör journalanteckningar sidoordnat som hanteras oskyddat under kortare eller

längre tid. Om sidoordnade anteckningar inte tillförs systemet eller förs in felaktigt och/eller ofullständigt innebär det risk för att journaler blir missvisande. Missvisande eller saknade journalanteckningar innebär bristande patient-/vårdtagarsäkerhet. I den omfattning detta sker upptäcks *inte* av en loggkontroll. Vi rekommenderar att kontroller som upptäcker det beskrivna förhållandet införs som ett komplement till loggkontrollerna.

- Andelen användaridentiteter som varit upplagda under granskningsperioden i förhållande till hur många som lämnat spår efter sig ha hanterat journalanteckningar för vårdtagare är 63 %. (428/673) Kan det vara rimligt att drygt var tredje användare vare sig har läst eller skrivit i journalen under denna tid? Vi rekommenderar att detta undersöks och att ändamålet med journalföring inte är oklart för de som fått behörighet att använda systemet.

- Inte vanligt men det förekommer personer med möjlighet att använda systemet under granskningsperioden som enligt information från PA-systemet då varit obehörig lärare och förskolelärare samt elevassistent och fritidspedagog. När användare inte är verksamma ska de inte ha behörighet till systemet. Här bör det säkerställas att det finns ändamålsenlig kommunikation mellan involverade ansvariga och/eller system så att både befattningar och tidsomfattningar av tjänsterna är korrekt angivna.

- Vi finner sammanlagt 16 testidentiteter i erhållen sammanställning av användare. Vårdgivaren ansvarar för att alla användare har en individuell behörighet. Detta innebär att endast personliga inloggningar är tillåtna och att inga så kallade gruppkonton får förekomma. Användarnas behörighet i vårdgivarens informationssystem måste vara anpassad till deras arbetsuppgifter. Vårdgivaren ansvarar också för att användarna tilldelas rätt behörighet, det vill säga tillräckligt för att de ska kunna utföra sina arbetsuppgifter på ett säkert sätt men samtidigt inte mer omfattande än vad som är nödvändigt. Att i detta sammanhang tillåta både anonyma och personanknutna testidentiteter i skarp miljö visar på en oacceptabel brist på kunskap i och därmed efterlevnad av de lagar som omgärdar journalhantering.

Ovanstående iakttagelser anser vi måste bilda principiell grund när urval görs för loggkontroller. När vi analyserar loggdata gör vi ytterligare iakttagelser som kan användas som underlag för urval. Nedan redovisas några exempel. Att en användare fångas av ett enstaka exempel motiverar kanske inte att vederbörande är en tydlig kandidat för en kontroll. En kombination av exempel som omfattar samma person gör däremot hen rimligtvis betydligt mer aktuell.

- Vår analysperiod innebär att loggen omfattar 308 kalenderdagar. Heltidsengagerade som har loggats för händelser på ett mycket stort respektive ett mycket litet antal datum inom den perioden torde vara kandidater för en kontroll.

- Vi noterar att det är 12 personer (2,8 %) som sammanlagt genererat drygt 50 % av alla loggrader under granskningsperioden. Om personens befattning och arbetsuppgifter inte motiverar att en stor mängd loggrader torde de vara aktuella för kontroll. Av de 12 är 7 sjuksköterskor och 5 är olika handläggare. Omvänt kan fråga ställas om *all* legitimerad personal skriver och läser journaldata i ändamålsenlig omfattning.

- 74 (17 %)användare är under granskningsperioden loggade för att endast ha tillfört och/eller läst data i en omfattning som genererat 10 loggrader eller färre. Har alla ett rimligt motiv för ett sådant enstaka behov?

- 15 användare som inte bedöms som legitimerade är loggade för mellan 50 och 137 rader på ett enskilt datum. Genomsnitt för alla 428 användare är 35 rader. Ett fåtal personer i en stor mängd sticker ut i jämförelse med andra. Detta är inte sällan ett motiv för en kontroll som klargör varför och avslöjar eventuellt felaktig användning av systemet.

- Risken för att eventuellt felaktigt ha utplånat journaldata redovisas i avsnitt ovan. Det är 40 stycken användaridentiteter som under analysperioden är loggade för händelsen ”Radera” och det på 1till 186 loggrader. Mycket få rader (0,4 %) utplånade av en relativt stor mängd användare är även framgent en indikation på att denna kontroll är rimlig att utföra.

- 40 användaridentiteter har tagit del av journaldata men inte tillfört någon. Ingen av dessa är legitimerad personal. Finns det bland de som endast läst under granskningsperioden som rimligen även ska ha tillfört data?

- Om man inte jobbar natt enligt PA-systemets anställningsuppgifter och ändå loggar merparten av raderna före 07:00 och efter 21:00 borde det vara en anledning till kontroll.

- Journaldata för 31 vårdtagare har under granskningsperioden hanterats av mellan 50 och 71 användare. Finns det professionella motiv för att alla användare per vårdtagare att ta del av journalanteckningarna?

- 63 användare (övervägande delen legitimerad personal och handläggare) har tagit del av journalanteckningar för mellan 50 och 629 vårdtagare. Finns det professionella motiv per användare för att ta del av journalanteckningar för respektive mängd av vårdtagare?

KPMG, dag som ovan

Lars Anteskog
Projektansvarig