Säters kommun

Revisorerna

2016-09-20

Kommunstyrelsen
Socialnämnden
Kommunfullmäktige för kännedom

Granskning av "Behörigheter och loggkontroll"

KPMG har av revisorerna i Säters kommun haft i uppdrag att granska hanteringen av behörigheter och åtkomstkontroll i kommunens datoriserade verksamhetsstöd avgränsat till Procapita HSL vid socialförvaltningens hälso- och sjukvårdsteam/Hemsjukvården.

Behörighetsstyrning och åtkomstkontroll är en viktig och central komponent i kommunens arbete med informationssäkerheten.

Från granskningen vill vi särskilt framhålla följande:

Det framgår otillfredsställande lite om vad som kommunövergripande gäller för informationssäkerheten inom området som denna granskning avgränsats till. Dokumenten baserar sig på föreskrifter och rekommendationer från lång tid tillbaka och från en myndighet som inte längre existerar. Övergripande och förvaltningsspecifikt styrdokument avseende informationssäkerhet står inte i vare sig praktisk och logisk relation till varandra. De refererar inte till varandra, skiljs åt av ålder och aktualitet. Mest oroväckande är att ansvarsförhållandena blir tvetydiga och därmed oklara.

Procapita HSL logg uppges ha kontrollerats på något sätt under vår granskningsperiod. Antalet kontrollerade och kontrollen i sig är vad vi förstår inte enligt de minimala och delvis felaktiga instruktioner som framgår av det enda verksamhetsspecifika styrdokument vi har erhållit.

Det är inte acceptabelt att det saknas en formaliserad och dokumenterad tilldelning av behörigheter. Kan vi inte granska användningen, ordningen, fullständigheten och riktigheten i behörigheterna kan heller inte verksamhetsansvariga säga att de har ändamålsenlig kontroll över att endast behöriga använder systemet. Behörighetstilldelningen är således vare sig säker eller ändamålsenlig.

Revisionen begär yttrande över bifogad rapport, inkluderande de åtgärder som ska vidtas och en tidplan för genomförande, senast 2016-12-15

De förtroendevalda revisorerna i Säters kommun

Enligt uppdrag

Bengt Wester

Lennart Hinders

Säters kommun

Behörigheter och loggkontroll

Revisionsrapport

KPMG AB
2016-09-20
Antal sidor: 12

Innehåll

1. Sammanfattning med kommentarer

Vi har av revisorerna i Säters kommun haft i uppdrag att granska hanteringen av behörigheter och åtkomstkontroll i kommunens datoriserade verksamhetsstöd avgränsat till Procapita HSL vid socialförvaltningens hälso- och sjukvårdsteam/Hemsjukvården. Behörighetsstyrning och åtkomstkontroll är en viktig och central komponent i kommunens arbete med informationssäkerheten.

Vi har granskat styrdokument, intervjuat samt analyserat data från Procapita (kontoinformation och loggar), anställningsdata från PA-systemet samt utdrag ur kommunens katalogtjänst (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:

Det framgår otillfredsställande lite om vad som kommunövergripande gäller för informationssäkerheten inom området som denna granskning avgränsats till. Dokumenten baserar sig på föreskrifter och rekommendationer från lång tid tillbaka och från en myndighet som inte längre existerar. I "SOSFS[1] 2008:14, Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården" ingår informationssäkerhetspolicy som ett centralt och viktigt dokument. Erhållna kommunövergripande styrdokument är inte i närheten av att bilda underlag för den styrning och dokumentation som granskad verksamhet kräver. Övergripande och förvaltningsspecifikt styrdokument avseende informationssäkerhet står inte i vare sig praktisk och logisk relation till varandra. De refererar inte till varandra, skiljs åt av ålder och aktualitet. Mest oroväckande är att ansvarsförhållandena blir tvetydiga och därmed oklara. Granskat verksamhetsområde visar med dokumentets innehåll att grundläggande kunskap finns om vad som krävs vad gäller styrning av informationssäkerhet inom området. Detta är ett viktigt dokument och ska därmed lyftas till beslut i en högre instans än till enskild tjänsteman. Systemansvarig torde vara verksamhetsansvarig vilket skulle innebära att om inte nämnden tar beslutet ska socialchef göra det. Ska kommunen som helhet lyckas med att åstadkomma ändamålsenlig informationssäkerhet krävs, inte endast för de områden som berörs i denna granskning, en genomgripande översyn av alla styrande dokument kommunövergripande likaväl som verksamhetsspecifika. (8.1 och 8.2)

Procapita HSL logg uppges ha kontrollerats på något sätt under vår granskningsperiod. Antalet kontrollerade och kontrollen i sig är vad vi förstår inte enligt de minimala och delvis felaktiga instruktioner som framgår av det enda verksamhetsspecifika styrdokument vi har erhållit. Styrdokumentet ("Dokument och Information") är en tjänstemannaprodukt och är inte beslutat av någon instans med övergripande ansvar för verksamheten. (8.3)

Det är inte acceptabelt att det saknas en formaliserad och dokumenterad tilldelning av behörigheter. Kan vi inte granska användningen, ordningen, fullständigheten och riktigheten i behörigheterna kan heller inte verksamhetsansvariga säga att de har ändamålsenlig kontroll över att endast behöriga använder systemet. Behörighetstilldelningen är således vare sig säker eller ändamålsenlig. Ansvariga ska inte tveka att omgående införa rutiner för att säkerställa behörighetstilldelningen och införa kontroller som regelbundet visar att den fungerar och efterlevs. (8.4)

[1] Socialstyrelsens författningssamling

Vi redovisar ett större antal rekommendationer baserat på vår analys av loggdata från Procapita. 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 Säters kommun haft i uppdrag att granska hanteringen av behörigheter och åtkomstkontroll i kommunens datoriserade verksamhetsstöd avgränsat till Procapita HSL vid socialförvaltningen.

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 socialförvaltningens hälso- och sjukvårdsteam/Hemsjukvård (Procapita HSL). 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.

6. Ansvarig styrelse

Granskningen avser kommunstyrelsen samt socialnämnden.

7. Metod

Granskningen har genomförts genom dokumentstudier och gruppintervju (2016-08-25) med nämndsekreterare, fd systemförvaltare Procapita, socialchef, biträdande socialchef, verksamhetschef HSL, verksamhetschef HSL äldreomsorg, systemadministratör HSL, medicinskt ansvarig sjuksköterska[2] och IT-chef. Utöver detta har BKS[3]-data från verksamhetssystem inhämtats för jämförelse med person- och anställningsregister samt vad som framgår av kommunens centrala katalogtjänst (AD[4]: et). Analysperiod har varit 2015-01-01 till 2016-03-31. Rapporten är faktagranskad av nämndsekreterare, fd systemförvaltare Procapita.

8. Granskningsnoteringar

Noteringarna redovisas avsnittsvis med kommentarer i samma ordning revisionsfrågorna anges under avsnittet syfte ovan. När vi skriver systemnamnet Procapita i denna rapport så avses endast systemets användning inom socialförvaltningens hälso- och sjukvårdsteam/Hemsjukvård.

---

[2] Medicinskt ansvarig sjuksköterska förkortas vanligtvis MAS

[3] BKS en förkortning av behörighetskontrollsystem.

[4] 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[5] och loggning?

Kommunen har en informationssäkerhetspolicy beslutad av kommunstyrelsen 2009-08-19. Dokumentet är upprättade enligt Krisberedskapsmyndighetens[6] rekommendationer om basnivå för IT-säkerhet (BITS[7]). Till policyn finns tre stycken konkretiserande instruktioner. En för vardera Kontinuitet och drift, Förvaltning samt Användare. De två första är daterade 2009-08-19 medan den för användare är daterad 2012-10-15. Av policyns inledning framgår att: *"... informationssäkerhetspolicy är en viktig del av Säters Kommun IT-verksamhet och redovisar ledningens viljeinriktning och stöd för informationssäkerhetsarbetet ... ".*

I instruktionen för Förvaltning avhandlas enligt policyn behörighetskontroll samt loggning och spårbarhet. När vi studerar dokumentet framgår om behörighet att: *"För att säkerställa att endast behöriga användare förekommer i informationssystemen ska beställning och borttagande av åtkomst till informationssystem ske på elektronisk blankett. Närmaste chef fyller i och skickar blanketten som bilaga i e-post till IT-enheten efter samråd med systemägare. Blanketten ska sparas hos både beställaren och IT-enheten. Samma blankett ska användas när konsulter eller andra utför arbete i informationssystem. Leverantörslösenord och behörigheter ska förvaras inlåsta."*

Om loggning sägs under rubriken *4.8 Övervakning* att:

- *Systemförvaltaren ansvarar för att loggarna analyseras en (1) gång per vecka*
- *Systemadministratören ansvarar för att loggarna rensas var tredje månad*
- *Loggarna ska sparas i fem (5) år*
- *Loggarna ska förvaras i en särskild katalog på kommunens server*
- *Detaljerad information samt anvisningar för användning och övervakning av loggfiler framgår av separat dokument.*

I bilaga 1 till informationssäkerhetsinstruktion Förvaltning exemplifieras arbetsgången avseende Procapita. Följande arbetsgång anges där *"rensningen ska utföras av tekniker p.g.a. att rensning ska åtföljas av kompress av CSS databas."*

- *Stäng Procapita servertjänst(er), Ciceron Service Manager*
- *Starta CSS i exklusivt läge med normal CSS-användare, via CCCToolBox*

---

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

[6] Krisberedskapsmyndigheten (KBM) var en svensk statlig förvaltningsmyndighet för frågor om samhällets säkerhet och ersatte när den inrättades 2002 Överstyrelsen för civil beredskap. Från 1 januari 2009 ersattes KBM av Myndigheten för samhällsskydd och beredskap (MSB).

[7] BITS en förkortning av "Basnivå för IT-säkerhet" utvecklas och stöds inte längre av MSB. Istället har det tillsammans med andra myndigheter utvecklats ett metodstöd för informationssäkerhet vilket syftar till att stödja organisationer som ska införa och tillämpa ett ledningssystem för informationssäkerhet, LIS.

- *Rensa "CSS logg" via CCCToolBox. Ange vilken period som ska rensas, t.ex. 2006 vilket innebär att hela 2006 rensas, välj 200611 om enbart november 2006 ska rensas. Har inga rensningar gjorts tidigare, rensa år för år, All rensning utförs innan kompress.*
- *Allt som rensas från CSS databas sparas till fil. Filen sparas i valfritt format. Efterfrågas filen, kan den startas i valfritt verktyg, t.ex. Excel.*
- *Komprimering av CSS databas sker via CCCToolBox. Observera utrymmeskraven.*
- *Tidsåtgång vid kontinuerlig rensning/kompress är 15 minuter. Rensning av ett helt år tar cirka 30 minuter.*

Även i instruktionen för Användare avhandlas behörighetskontroll. Där anges att:

- *Din chef lämnar en skriftlig beställning (ej muntligt) till systemförvaltare och IT enheten efter samråd med systemägare*
- *IT enheten och systemförvaltare lägger till dina behörigheter*
- *Du kvitterar din behörighet genom att du får en kopia på beställningen*

Kommentar

De dokument som övergripande styr informationssäkerheten i kommunen baserar sig på föreskrifter och rekommendationer från lång tid tillbaka och från en myndighet som inte längre existerar. I "SOSFS[8] 2008:14, Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården" ingår informationssäkerhetspolicy som ett centralt och viktigt dokument. Erhållna kommunövergripande styrdokument är vad gäller behörighetshanteringen inte orimliga i sina krav på ansvariga och användare. Med hänvisning till SOSFS 2008:14 är däremot det som sägs om loggning felaktigt vad gäller hur lång tid den ska sparas. Det är tio år som gäller.

Alla omnämnda styrdokument ovan anses till viss del föråldrade och behöver i varierande omfattning och anledning uppdateras om inte ersättas. Omvärldsförändringar, externa regler, behov av faktakomplettering, teknisk utveckling etc. motiverar en sådan genomgång. Vad vi förstår pågår ett sådant arbete men inte i den omfattningen och enligt en tidplan att resultatet varit gällande för denna granskning.

8.2 Särskilda anvisningar för behörighetstilldelning och loggkontroll

I socialförvaltningens ledningssystem för kvalitet finns ett dokument benämnt "Dokumentation och Information". Dokumentet gäller från 2015-04-01 är reviderat av MAS. Av dokumentet framgår inledningsvis: *"Legitimerad personal har ett personligt ansvar för att föra patientjournal och därför ska det alltid framgå av vem och när uppgifterna har dokumenterats. Journalen är även ett arbetsinstrument för hälso- och sjukvårdspersonalen. Endast den legitimerade personal som är direkt inblandad i vården av den enskilde har rätt att ta del av en journalhandling. Omvårdnadspersonalen har rätt att i samråd med sjuksköterska, sjukgymnast och arbetsterapeut ta del av vissa delar i dokumentationen som avser patientens omvårdnad."*

[8] Socialstyrelsens författningssamling

Under rubriken Ansvar framgår att socialnämnden utser *"person eller personer som ska ansvara för informationssäkerhetsarbetet."* Verksamhetschef ansvarar bland annat för att:

- *Utdelade behörigheter stämmer överens med befattningshavarens arbetsuppgifter.*
- *Följa upp informationssystemets användning genom regelbunden kontroll av loggarna*

Under rubriken "Informationssäkerhet datajournaler" framgår i avsnitt nedan om behörighetshantering och loggkontroll (Kontroll av åtkomst till patientuppgifter)

8.2.1 Behörigheter

- *Nätverkskonto och ny användare i Procapita beställs hos Systemförvaltare HSL, efter samråd med Verksamhetschef HSL. Huvudsystemansvarig informeras på särskild blankett.*
- *Systemförvaltare HSL ansvarar för att tilldela individuella behörigheter i Procapita.*
- *Systemförvaltare HSL ansvarar för SITSH kort tillsammans med huvudsystemförvaltaren och HSA katalogen kontrolleras en gång i månaden.*
- *Verksamhetsområdeschef för HSL personal ansvarar för att meddela Systemförvaltare - HSL förändringar i tjänst eller avslutad anställning så denne kan avsluta kontot och informera huvudsystemansvarig.*
- *Uppföljning av behörigheterna skall ske halvårsvis i september och mars av Systemförvaltare - HSL.*

8.2.2 Kontroll av åtkomst till patientuppgifter

Genom loggning skall det framgå vilka åtgärder som vidtagits med patientuppgifterna, även tidpunkt, enhet, användarens och patientens identitet ska framgå. Systematiska kontroller skall göras av Systemförvaltare HSL.

- *Minst två personer ska varje månad kontrolleras och under året ska all HSL-personal ha blivit kontrollerad.*
- *Genomförda kontroller av loggar dokumenteras i pärm på kontoret på Jönshyttevägen 1.*
- *Loggarna sparas i minst 10 år.*

Kommentar

Övergripande och förvaltningsspecifikt styrdokument (instruktioner) avseende informationssäkerhet står inte i vare sig praktisk eller logisk relation till varandra. De refererar inte till varandra, skiljs åt av ålder och aktualitet. Mest oroväckande är att instruktioner, funktioner och ansvarsförhållandena blir tvetydiga och därmed oklara. Inom granskat verksamhetsområde visas med dokumentets innehåll att viss grundläggande kunskap finns om vad som krävs vad gäller styrning av informationssäkerhet inom det område som granskas. Detta är ett viktigt dokument och ska därmed lyftas till beslut i en högre instans än till enskild tjänsteman. Systemansvarig torde vara verksamhetschef HSL vilket skulle innebära att om inte nämnden tar beslutet ska socialchef göra det som system-

ägare. Ska kommunen som helhet lyckas med att åstadkomma ändamålsenlig informationssäkerhet krävs, inte endast för de områden som berörs i denna granskning, att den kommunövergripande översynen som uppges pågå även inkluderar verksamhetsspecifika styrdokument.

8.3 Kontroll av loggar och internkontroll

Enligt uppgift så har inga kontroller utförts under granskningsperioden. Gruppintervjun indikerar dock att någon form av kontroll har utförts. Hur och när kontrollarbetet i detalj har utförts sedan dokumentet upprättades i januari 2014 finns inte dokumenterat. Vad vi erfar har inte informationssäkerhet i allmänhet och loggkontroll i synnerhet funnits med som kontrollmål i internkontrollplanen för 2015.

Kommentar

Systematisk logguppföljning 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. Insikten om detta framgår av "Dokumentation och Information". I det sammanhanget är det då otillfredsställande att kommunen under lång tid underlåtit att utföra kontroller, som alla ansvariga känner till, av hur journaldata används och hanteras. Granskad verksamhet har därmed under lång tid inte följt vare sig lag, förordningar eller interna styrdokument. Vår enda rekommendation är att detta skyndsamt åtgärdas. Grundkunskapen finns och all data som behövs går att göra tillgänglig med den samlade kunskap som finns i kommunen. Det som krävs är initiativkraft kanaliserad till en mindre projektgrupp under styrning av verksamhetsledningen.

De som arbetar inom granskat område bedömer vi inte är omedvetna om vad som krävs. Att då endast utgå från det som beskrivs i "Dokumentation och Information" bedöms inte vara ändamålsenligt. Beskriven urvalsmetod och utförande anser vi även ska utsättas för en ny riskbedömning. Utöver att i riskanalysen utvärdera innevarande rutin anser vi att det finns starka motiv att tillföra ytterligare instruktioner och metoder så att loggkontrollen ska kunna bedömas vara ändamålsenlig.

Vi exemplifierar med några rekommendationer till förbättring:

- Alla som använder systemet över en given tidsperiod ska omfattas av kontroll, även chefer, controllers, verksamhetsextern personal, konsulter om sådana används etc.
- Urvalmetodiken ska vara sådan att analyserbara indikationer används så att även riskbeteenden ligger till grund för urvalet.
- Om stickprov och slump ska användas som urvalsmetod ska den vara statistiskt säkerställda och representativ för populationen av loggade personer.

- Beakta vad Datainspektionen skriver på sin hemsida. *"Bestäm med vilken omfattning (antal och tidsintervall) logguppföljningen ska ske. Eftersom det inte enbart är antalet loggposter vid logguppföljningen 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 av loggdata över tid ska göras på samma sätt och på samma grunder oavsett vem som utför den. Bedömningsgrunderna behöver vara detaljerade och finnas dokumenterade.

- Det ska framgå hur en kontrollerad användare kan få utförd kontroll överprövad.

- 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 får lämnas ut.

- Av "SOSFS[9] 2008:14. Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården" framgår att loggar likaväl som loggkontroller ska sparas i 10 år. Det måste finnas dokumenterade processer/rutiner som säkerställer att så sker och att informationen under denna tid inte kan förändras eller förstöras. 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 (en aktivitet i ett LIS[10]) 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).

I avsnittet 8.5 nedan redovisar vi ett antal iakttagelser av genomgången av 1 086 147 loggrader omfattande perioden från 2015-01-01 till 2016-03-31. Vi rekommenderar att även dessa iakttagelser beaktas i analysarbetet och får påverka nya/uppdaterade instruktioner och rutiner.

8.4 På vems verksamhetsansvar har behörigheter hanterats?

För att få behörighet till Procapita HSL krävs i Säters kommun *inte* en administrativ åtgärd som ska dokumenteras på en blankett. Att en blankett ska användas framgår av styrdokumentet "Dokumentation och Information". Blanketten är inte använd de senaste åren.

Vad vi förstår har inte IT-kontorets personal eller personal från annan förvaltning tillgång till Procapita HSL via det ordinarie användargränssnittet. Sekretessavtal med externa konsulter som på något sätt kan få tillgång till data i Procapita HSL finns inte upprättade.

[9] Socialstyrelsens författningssamling

[10] Ledningssystem för informationssäkerhet

Rådande förhållanden gör att vi *inte* haft underlag för att granska om:

- Det saknas blanketter för aktiva användare. Speciellt för de som förekommer i loggen.
- Det framgår vilken typ av behörighet användaren skall ha för sin respektive roll.
- Blanketter alltid är underskrivna eller på annat sätt är godkända av överordnad.
- Blanketterna har använts vid ändring och avveckling.
- Det kan finnas användare som erhållit fler än en användaridentitet.
- Det finns användare som getts behörigheter trots att de inte förekommer som anställda och/eller förekommer i AD: et.
- Blanketter finns som ger kommun-/verksamhetsexterna tillgång till systemet.

Kommentar

Det är inte acceptabelt att det saknas en formaliserad och dokumenterad tilldelning av behörigheter. Kan vi inte granska användningen, ordningen, fullständigheten och riktigheten i behörigheterna kan heller inte verksamhetsansvariga säga att de har ändamålsenlig kontroll över att endast behöriga använder systemet. Behörighetstilldelningen är således vare sig säker eller ändamålsenlig. Ansvariga ska inte tveka att omgående införa rutiner för att säkerställa behörighetstilldelningen och införa kontroller som regelbundet visar att den fungerar och efterlevs.

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 skall även vara tidsbegränsade. Under längre bortovaro skall de avaktiveras alternativt avvecklas. Redan vid rollsättning och behörighetshanteringen måste det säkerställas att möjligheten att totalt avlägsna journalanteckningar (HSL-text) ges med mycket stor restriktivitet. Inte minst för system som Procapita är det utomordentligt viktigt att det finns instruktioner som innebär stor restriktivitet i tilldelning av databasåtkomst. Det skall 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:

- 1 086 147 loggrader från Procapita.
- Kontodata för 394 användare av Procapita.
- 298 användaridentiteter förekommer i loggen.

- 1 566 personers anställningsdata i PersonecP (kommunens PA-system).
- 2 257 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. Iakttagelser och kommentarer redovisas under samma punkt i avsnittet nedan.

Från jämförelser med bäring på användare av Procapita noterar vi följande:

- Vi identifierar personer i PA-systemet som med ledning av angiven benämning/kategori (undersköterskor och vårdbiträden) rimligen borde ha en identitet registrerad 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-/brukarsäkerhet. I den omfattning detta sker upptäcks inte av en loggkontroll på det sätt den idag föreskrivs. Vi rekommenderar att kontroller som upptäcker det beskrivna förhållandet införs som ett komplement till övriga loggkontroller.
- Det är inte alla registrerade i systemet som gör avtryck i loggen genom att under granskningsperioden ha sparat och/eller läst. Det är nästan etthundra användare, mestadels undersköterskor och vårdbiträden men även legitimerad personal och chefer förekommer. Det finns mest troligt flera anledningar till detta förhållande. Vi rekommenderar att anledningarna identifieras och att det säkerställs att förhållandet inte negativt påverkar verksamhetens uppdrag.
- Vår analysperiod innebär att loggen omfattar 456 kalenderdagar. Vi finner att 10 identiteter skrivit och/eller läst journaldata 270 till 289 dagar. 54 har gjort detsamma för fem eller färre dagar. Heltidsengagerade och tillsvidareanställda som oavsett kategori har loggats på ett mycket stort respektive ett mycket litet antal datum under femton månader torde vara kandidater för kontroll.
- Vi noterar att det är 19 användare (6 %) som sammanlagt genererat drygt 50 % av alla loggrader under femton månader. Om användarens befattning och arbetsuppgifter inom den mängden inte motiverar en så stor mängd loggrader torde den vara aktuella för kontroll.
- Åtta (8) personer är loggade för mellan 505 och 1 231 rader på ett enskilt datum. Tio (10) har i genomsnitt över 100 loggrader eller fler räknat på det antal dagar de loggats. 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.
- Aktiviteten "Tagit bort" används av sammanlagt 53 användare. Alla är legitimerad personal, chef eller administratör. Majoriteten av genererade loggrader härrör från en administratörs borttagningar av bevakningar vid två tillfällen 2015, 26 maj och 22 december.

Vilken kontroll finns att övriga 52 användare åsatts en roll (därmed behörighet) som innebär att borttaget inte omfattar patientuppgifter som ska kvarstå efter en rättning?

- Finns det personer bland de 19 som endast läst journaluppgifter under femton månader som rimligen även ska ha sparat sådana? I detta fall mestadels undersköterskor som enligt arbetsuppgifter och behörighet ska göra journalanteckningar.

- 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.

- Att det framför allt är legitimerad personal tillsammans med administratörer och chefer som skriver och läser journalanteckningar för flest antal brukare under femton månader bedöms som rimligt. De femtio (50) som tagit del av journaldata för flest brukare har hanterat journaldata för mellan 151 och 1 498 stycken. Det är föga förvånande att systemadministratörer och biståndshandläggare toppar den listan. Fjorton (14) av de 50 är undersköterskor och vårdbiträden som har hanterat journaldata för mellan 151 och 227 brukare. För dessa borde det vara rimligt att det finns en motiverad anledning till behovet. Detta eftersom snittet för dessa kategorier är 53 brukare. Kategorierna använda i jämförelsen är yrkesrollerna så som de anges i systemet. För urval till kontroller anser vi att det ska tas hänsyn till denna typ av indikationer.

- De femtio (50) brukare vars journaldata har hanterats av flest antal användare varierar från 82 till 110 stycken per brukare. Det är rimligt att förvänta sig väl motiverade skäl till att ett så stort antal användare behöver journaldata för omvårdnad av en enskild brukare. Med underlag av de 110 användare som hanterat journaldata för en (1) brukare noterar vi att 33 enligt angiven benämning är legitimerad personal tillsammans med administratörer och chefer. Det är rimligt att detta exempel på iakttagelse från loggen ska användas när urval för kontroll görs. Vilka motiv finns för att 77 användare i övrigt tagit del av journalen för en enskild brukare?

Ovanstående iakttagelser anser vi kan bilda principiell grund när urval görs för loggkontroller. Enstaka exempel motiverar kanske inte ett urval. En kombination av exempel som omfattar samma användare gör hen rimligtvis betydligt mer aktuell för en kontroll.

KPMG, dag som ovan

Lars Anteskog
Projektansvarig