Nora kommun
Revisorerna

2016-08-25

Till
Kommunstyrelsen

För kännedom
Kommunfullmäktige

Granskning avseende hanteringen av behörigheter och loggkontroll i kommunens datoriserade verksamhetsstöd som hanterar hälso-, sjukvård och social omsorg

På vårt uppdrag har KPMG genomfört en granskning avseende hanteringen av behörigheter och loggkontroll i kommunens datoriserade verksamhetsstöd som hanterar hälso-, sjukvård och social omsorg. I det senare omfattas *inte* individ och familjeomsorgen. Uppdraget ingår i revisionsplanen för år 2016.

Granskningen visar på brister i styrning och kontroll inom området. Resultatet av de registeranalyser som genomförts visar på brister avseende hanteringen av behörigheter och loggkontroll och den pekar även på risker och omständigheter som kommunen bör uppmärksamma och följa upp.

Vi anser att en genomgripande översyn bör göras av alla styrande dokument kommunövergripande likaväl som verksamhetsspecifika avseende informationssäkerhet.

Vi bedömer det som oacceptabelt att det *inte* finns en rutin/process formaliserad och dokumenterad för tilldelning, förändring och avveckling av behörigheter. Detta är en brist som snarast ska åtgärdas.

Vi anser det mycket otillfredsställande att kommunen under lång tid underlåtit att utföra kontroller av hur journaldata används och hanteras. Granskad verksamhet har därmed under lång tid inte följt vare sig lag, förordningar eller interna styrdokument. Vår rekommendation är att detta skyndsamt åtgärdas.

Revisionen vill ha svar av kommunstyrelsen senast den 30 november 2016 på vilka åtgärder de har för avsikt att vidta med anledning av ovanstående synpunkter samt vad som i övrigt framkommer i bifogad revisionsrapport.

För revisorerna i Nora kommun

Jan Kallenbäck
Ordförande i revisionen

Nora kommun

Behörigheter och loggkontroll

Revisionsrapport

KPMG AB
2016-08-25
Antal sidor: 12

Innehåll

1. Sammanfattning med kommentarer

Vi har av revisorerna i Nora kommun haft i uppdrag att granska hanteringen av behörigheter och åtkomstkontroll i kommunens datoriserade verksamhetsstöd avgränsat till socialtjänstens system Vivas HSL-data. Behörighetsstyrning och åtkomstkontroll är en viktig och central komponent i kommunens arbete med informationssäkerheten.

Vi har granskat styrdokument, intervjuat samt analyserat data från Viva (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 informationssäkerhet. 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. Verksamhetsområdet Välfärd visar med dokumentets innehåll att 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 verksamhetsansvarig vilket skulle innebära att om inte utskottet 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)

Vi bedömer det som oacceptabelt att det *inte* finns en rutin/process formaliserad och dokumenterad för tilldelning, förändring och avveckling av behörigheter. Detta är en brist som snarast ska åtgärdas. Det ska aldrig råda tvivel på vems ansvar en enskild användare getts vilken behörighet att använda systemet. Det är i sammanhanget lika viktigt för den enskilda användaren att känna sig trygg i att endast ha de behörigheter som följer av roll och ansvar. Funktionsanvändare (om och när sådana används), konsulter, temporära användare och uppdragstagare ska omfattas av samma formaliserade hantering som anställda vad gäller behörighetstilldelning. Sekretessavtal med externa an vändare ska upprättas på individnivå. (8.4)

[1] Socialstyrelsens författningssamling

Systematisk logguppföljning görs primärt för att brukaren ska känna sig trygg med att personal inte tar del av information som denne inte är behörig till. De som arbetar inom området hälso- och sjukvård bedömer vi är väl medvetna om detta förhållande. Det är då mycket otillfredsställande att kommunen under lång tid underlåtit att utföra kontroller 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 utan externt konsultstöd. Det som krävs är initiativkraft kanaliserad till en mindre projektgrupp under styrning av verksamhetsledningen. Utöver att utvärdera innevarande inte använda rutin anser vi att det finns starka skäl att tillföra ytterligare instruktioner och metoder så att loggkontrollen ska kunna bedömas vara ändamålsenlig. Som exempel redovisar vi i rapporten ett större antal rekommendationer baserat på vår analys av loggdata. Enstaka exempel motiverar kanske inte ett urval. En kombination av rekommendationer som omfattar samma användare gör dock rimligtvis hen betydligt mer aktuell för en kontroll. (8.3 och 8.5)

2. Bakgrund

Vi har av revisorerna i Nora kommun haft i uppdrag att granska hanteringen av behörigheter och loggkontroll i kommunens datoriserade verksamhetsstöd som hanterar hälso-, sjukvård och social omsorg. I det senare omfattas *inte* individ och familjeomsorgen. Verksamheternas utveckling i en kommun har med åren blivit alltmer IT-beroende vilket innebär nya former av hot, risker men även möjligheter. 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 verksamhetsområde Välfärd inom Kommunförvaltningen (Viva). 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 socialutskottet och genom uppsynsplikten kommunstyrelsen.

7. Metod

Granskningen har genomförts genom dokumentstudier och intervjuer med systemadministratör och medicinskt ansvarig sjuksköterska[2]. Utöver detta har BKS[3]-data från Viva inhämtats för jämförelse med person- och anställningsregister samt vad som framgår av kommunens centrala katalogtjänst (AD[4]: et). Granskningsperiod har varit från 2015-01-01 till 2016-03-31.

Uppdraget och rapporten i utkastform är presenterad och förklarad vid en sammankomst i Nora 2016-06-09. Närvarande var tf socialchef, systemadministratör, medicinskt ansvarig sjuksköterska, personalchef, enhetschef hälso- sjukvård och rehabilitering, It-tekniker samt en revisor från kommunrevisionen. Rapporten är därefter faktagranskad av systemadministratören och medicinskt ansvarig sjuksköterska.

8. Granskningsnoteringar

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

[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?

Under granskningsperioden saknar kommunen en övergripande informationssäkerhetspolicy. Däremot finns det ett dokument som benämns ”Systemsäkerhetsplan för IT-infrastruktur” och ett benämnt ”IT-säkerhetsinstruktion Användare”. Båda dokumenten är tillämpningsföreskrifter till en IT-säkerhetspolicy. Dokumenten är upprättade enligt Krisberedskapsmyndighetens[6] rekommendationer om basnivå för IT-säkerhet (BITS[7]). IT-säkerhetspolicyn är antagen av kommunfullmäktige 2006-04-26. Planen och instruktionen är antagen av kommunstyrelsen. Systemsäkerhetsplanen är senast reviderad 2014-02-06.

Av ”Systemsäkerhetsplan för IT-infrastruktur” framgår i bilaga 2 ”Återstående åtgärder” under rubriken ”Kommungemensam rutin för hantering av behörigheter” att: *”Problem då många verksamhetssystem levereras med inbyggda rutiner som inte kan förändras av IT-enheten. Eventuellt kan sådana rutiner skötas via en Metakatalog.”*

Av ”IT-säkerhetsinstruktion Användare” framgår under rubriken ”Behörighet” att: *”IT-systemen är utrustade med behörighetskontrollsystem för att säkerställa att endast behöriga användare kommer åt information. De behörigheter du blir tilldelad beror på arbetsuppgiften och avgörs av verksamhetsansvarig. Vikarier och tillfällig personal som tilldelas behörigheter, skall ha en tidsbegränsning inlagd i systemen som motsvarar anställningstiden.”* Av ”Bilaga 1: Klassning av information:” framgår att: *”Nora kommun har idag inget dokumenthanteringssystem som stödjer ovanstående (*informations*)klassning, men man ska ha klassningen i åtanke när man arbetar med dokument.”*. I bilaga 3 framgår hur elektronisk information får lagras.

Kommentar

Det framgår otillfredsställande lite om vad som kommunövergripande gäller för informationssäkerhet. Dokumenten 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 inte i närheten av att bilda underlag för den styrning och dokumentation som granskad verksamhet kräver. Alla omnämnda styrdokument ovan är i ursprunget tio år gamla och behöver i varierande omfattning och anledning uppdateras om inte ersättas. Omvärldsförändringar, externa regler, behov av faktakomplettering, teknisk utveckling etc. motiverar en sådan genomgång.

[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 utvecklat ett metodstöd för informationssäkerhet vilket syftar till att stödja organisationer som ska införa och tillämpa ett ledningssystem för informationssäkerhet, LIS.

[8] Socialstyrelsens författningssamling

8.2 Särskilda anvisningar för behörighetstilldelning och loggkontroll

Socialförvaltningen har i princip endast ett styrdokument som styr och vägleder inom hälso- och sjukvården, ”Riktlinjer för kommunal hälso- och sjukvård informationshantering och journalföring”. Upprättad av MAS[9] 2012-01-23. Med bäring på denna granskning framgår följande av dokumentet:

Inledningsvis sägs: Vårdgivaren har ett ansvar för att det i verksamheten finns ett ledningssystem för kvalitet och patientsäkerhet. I ledningssystemet ska det finnas angivet vem som har ansvar för vad runt informationshantering och journalföring inom hälso- och sjukvård. Med vårdgivare menas Nora kommun. Verksamhetschef för HSL är socialchefen. Vidare anges bland annat att: Det skall finnas en informationssäkerhetspolicy som säkerställer tillgänglighet, riktighet, sekretess och spårbarhet av patientuppgifter. I kommunen är det systemansvarig för Viva som ansvarar för informationssäkerhetsarbetet. Uppföljningen av informationssystemets (Viva) användning ska utföras genom regelbunden kontroll av loggarna.

8.2.1 Behörighetstilldelning

Under rubriken ”Styrning av behörigheter” framgår bland annat att:

- *”Vårdgivaren ska bestämma villkor för åtkomst till patientuppgifter samt upprätta rutiner för tilldelning, förändring, borttagning och regelbunden uppföljning av behörigheter”*. Några sådana har vi inte kunnat ta del av.
- *”… en plan för styrning av behörigheter (ska) utarbetas”*. Någon plan finns inte upprättad.
- *”Varje användare ska tilldelas en individuell behörighet för åtkomst till patientuppgifter. Vårdgivarens beslut om tilldelning av behörighet ska föregås av en behovs- och riskanalys.”* Underlag för analys saknas och den enligt uppgift har någon sådan aldrig utförts.
- *”De som tilldelats behörigheter ska ges såväl muntlig som skriftlig information om grundläggande regler för åtkomst till vårddokumentation”*.

8.2.2 Loggkontroll

Under rubriken ”Kontroll av åtkomst till patientuppgifter” framgår bland annat att:

- *Systematiska och återkommande stickprovskontroller av loggarna* ska göras.
- *”Genomförda kontroller av loggarna dokumenteras och sparas i minst 10 år.”*
- *”Om det vid loggningskontroll framkommer att någon tagit del av uppgifter som personen inte haft behörighet till ska arbetsrättslig åtgärd och/eller polisanmälan ske.”*

[9] Medicinskt ansvarig sjuksköterska.

I bilaga 1 ”Instruktion inför journalgranskning av dokumentation inom kommunal hälso- och sjukvård” till dokumentet framgår detaljer om målet, metoden, urvalskriterier, utförande och hur resultatet av en journalgranskning skall hanteras. En motsvarande detaljerad instruktion för loggkontroller finns inte.

Kommentar

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. Inom verksamhetsområde Välfärd visar med dokumentets innehåll att 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 verksamhetsansvarig vilket skulle innebära att om inte utskottet 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.

8.3 Kontroll av loggar

Loggkontrollarbetet styrs inte av några dokumenterade detaljerade beskrivningar Vad vi förstår så har några sådana aldrig framställts. Enligt uppgift så har heller inga loggkontroller utförts under den granskningsperiod som gällt för uppdraget.

Kommentar

Det är mycket otillfredsställande att kommunen under lång tid underlåtit att utföra kontroller 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, all data som behövs går att göra tillgänglig utan externt konsultstöd. Det som krävs är initiativkraft kanaliserad till en mindre projektgrupp under styrning av verksamhetsledningen.

De som arbetar inom granskat område bedömer vi är medvetna om vad som krävs. Att då ensidigt utgå från den metodik som beskrivs i ”Riktlinjer för kommunal hälso- och sjukvård informationshantering och journalföring” bedöms inte vara ändamålsenligt. Att i kontrollerna inte ta hänsyn till riskerna med att systemet saknar spärrmöjlighet mellan olika lagrum indikerar att det snarast behöver genomföras en riskanalys som tar hänsyn till detta och att resultatet får påverka utformningen av framtida kontroller. 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 skäl 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, kommunexterna sjukgymnaster, konsulter 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[10] 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[11]) 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 1 638 150 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.

[10] Socialstyrelsens författningssamling

[11] Ledningssystem för informationssäkerhet

8.4 På vems verksamhetsansvar tilldelas behörigheter?

Det finns inga dokumenterade rutiner för behörighetsadministrationen. Initialt lades användare upp från listor utan information om vem som var ansvarig för vem. I det skedet medverkade även systemleverantören till att användare lades upp. På senare tid görs merparten av beställningarna via mail. Vid granskningstillfället tillämpas en metod som innebär ett samarbete mellan IT-enheten och systemadministratören så att åtkomst till Viva inte erhålls med mindre än att personen finns registrerad i PA-systemet och i kommunens AD. Trots detta noterar vi brister men även möjlighet till speciella upplägg. Det senare gäller sjukgymnasterna som alla är anställda av landstinget och då hanteras som kommunexterna användare. Den vanligast förekommande bristen vi noterat är att informationen i Viva, i PA-funktionen och hos IT-enheten inte alltid är densamma.

Vi har inte kunnat säkerställa att kommunen i sin ägo har ett sekretessavtal med systemleverantören. Vi kan notera att anställda hos systemleverantören, om än inte i någon större omfattning och inom avgränsningen för denna granskning, både läst och skrivit journalanteckningar.

Kommentar

Vi bedömer det som oacceptabelt att det inte finns en formaliserad och dokumenterad rutin/process för tilldelning, förändring och avveckling av behörigheter. Detta är en brist som snarast ska åtgärdas. Det ska aldrig råda tvivel på vems ansvar en enskild användare getts vilken behörighet att använda systemet. Det är i sammanhanget lika viktigt för den enskilda användaren att känna sig trygg i att endast ha de behörigheter som följer av roll och ansvar.

Sekretessavtal med externa användare ska upprättas på individnivå. Det är svårt för kommunen att upprätthålla en kontroll av att kommunexterna användare över tid alltid har sekretessavtal med sina anställda som överensstämmer med de krav kommunen över tid har på sina anställda. I samband med att individuella avtal upprättas bör det även göras en översyn av hur många konsulter som behöver ha tillgång till kommunens produktionsdata.

Funktionsanvändare (om och när sådana används), konsulter, temporära användare och uppdragstagare ska omfattas av samma formaliserade hantering som anställda vad gäller behörighetstilldelning. 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.

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:

- 1 638 150 loggrader från Viva.
- Kontodata för 780 användaridentiteter [12]upplagda som användare av Viva.
- Av de 780 identiteterna kan med underlag av uppgifter i kontodata[13] 693 identifieras som användare i någon omfattning av HSL-delen av systemet.
- Av de 693 identiteternas kan vi via vad som anges som för- och efternamn notera att 518 identiteter förekommer i loggen.
- 2 040 personers (baserat på angivet personnummer) anställningsdata i PersonecP (kommunens PA-system).
- 4 352 identiteter i AD: et. Fördelat på 1 271 i den administrativa delen och 3 081 i skoldelen.

Iakttagelser och kommentarer från våra jämförelser redovisas i punkterna nedan. De fyller två syften genom att beskriva potentiella brister och därmed även bilda principiell grund när urval görs för loggkontroller. Enstaka exempel motiverar kanske inte ett urval. En kombination av exempel som omfattar samma person/identitet gör hen rimligtvis betydligt mer aktuell för en kontroll.

- Vi identifierar personer i PA-systemet som med ledning av angiven/benämning/kategori (mestadels undersköterskor och vårdpersonal men även sjuksköterska) borde ha en identitet registrerad i Viva men har inte 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.
- Vi använder personnumret (och namnet eftersom personnumret inte fullständigt förekommer i AD och som identifikation av Vivaanvändare) som jämförelseparameter och finner i Viva 17 användaridentiteter som *inte* går att återfinna i erhållen anställnings- och AD-data. Fem av dessa 17 återfinns även i loggdata. Vi rekommenderar att det regelbundet kontrolleras att personer med behörigheter i Viva finns förtecknade som anställda eller

[12] Beräknat på antalet så kallade kortnamn.

[13] Enligt uppgift så är personer angivna med en så kallad profession angiven upplagda som användare av HSL-delen.

uppdragstagare och i övrigt med korrekta uppgifter i kommunens PA-system. Om en person inte längre har en anställning ska den inte heller förekomma som aktiv i AD: et.

- Vår analysperiod innebär att loggen omfattar 456 kalenderdagar. Vi finner att 22 identiteter skrivit och/eller läst journaldata 231 till 278 dagar. 74 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 35 personer som sammanlagt genererat drygt 50 % av alla loggrader (skrivit eller läst journaldata) under femton månader. Om personens kategori och arbetsuppgifter inte motiverar en stor mängd loggrader torde de vara aktuella för kontroll.

- Vi noterar å andra sidan att det är 282 personer som sammanlagt genererat drygt 10 % av alla loggrader (skrivit eller läst journaldata) under femton månader. Om personens kategori och arbetsuppgifter inte motiverar en så liten mängd loggrader torde de vara aktuella för kontroll. Av de 282 så har 23 stycken i snitt genererat en eller färre rader per månad. Vad motiverar (även ekonomiskt) att dessa är registrerade som användare av systemet?

- Åtta (8) personer genererar mellan 304 och 702 rader avseende läsning av journalanteckningar på ett enskilt datum. Fyra (4) av dessa är legitimerad personal eller systemadministratör. Elva (11) personer har i genomsnitt genererat över 50 loggrader eller fler räknat på det antal dagar de loggats. Här är sju legitimerad personal eller systemadministratör. Den sistnämnda iakttagelsen bedöms som rimligare att förvänta sig än den första. Ett fåtal personer i en stor mängd sticker här ut i jämförelse med andra. Detta är inte sällan ett motiv för en kontroll som klargör varför och avslöjar eventuellt felaktig användning av systemet.

- Sjutton (17) personer som under 15 månader totalt läst fler än 100 rader har på ett enskilt datum läst tre till åtta så många rader som på det datum då de läste näst flest rader. Ingen av dessa är legitimerad personal. Återigen ett fåtal personer i en stor mängd sticker ut genom att läsa merparten av journalanteckningarna på ett enskilt datum. Detta är inte sällan ett motiv för en kontroll.

- Under 15 månader har sex läst men inte skrivit i journalen. En har skrivit men inte läst. Hur rimligt är det att en användare endast skriver eller läser journalanteckningar?

- Att det framför allt är legitimerad personal tillsammans med handläggare och chefer som skriver och läser journalanteckningar för flest antal brukare under femton månader bedöms som rimligt. De femtio (50) i dessa kategorier som tagit del av journaldata för flest brukare har hanterat journaldata för mellan 139 och 1 299 stycken. Det är föga förvånande att handläggarna toppar den listan. Sexton (16) av de 50 är undersköterskor och biträden som har hanterat journaldata för mellan 142 och 274 brukare. För dessa borde det vara rimligt att det finns motiverad anledning till behovet. Detta eftersom snittet för dessa kategorier är 37 brukare. Kategorierna använda i jämförelsen är yrkesrollerna så som de anges i Viva. 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 76 till 121 stycken per brukare. Det är rimligt att förvänta sig väl motiverade skäl till att så många behöver journaldata för omvårdnad av en enskild brukare. Med underlag av de 121

användare som hanterat journaldata för en (1) brukare noterar vi att 39 enligt angiven yrkesroll i Viva är legitimerad personal tillsammans med handläggare och chefer. Det är rimligt att detta exempel på iakttagelse från loggen ska användas när urval för kontroll görs. Vilka motiv finns för att 82 inte legitimerade användare tagit del av journalanteckningarna för en enskild brukare?

- 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. Vi anger inget antal här då vi inte känner oss säkra på att PA-systemet är fullständigt uppdaterat med de som faktiskt någon gång har sin arbetstid förlagd till natt.

- Vi noterar att personal från ILAB både läser och gör någon form av journalanteckningar om än i verksamheter utanför avgränsningen för denna granskning. Av det följer att även extern personal ska omfattas av loggkontroll.

KPMG, dag som ovan

Lars Anteskog
Projektansvarig