LANDSTINGSREVISIONEN

Granskning av behörigheter till journalsystemet

Rapport nr 18/2015

VÄSTERBOTTENS LÄNS LANDSTING

Februari 2016
Jonas Hansson, revisionskontoret
Diarienummer: REV 61:2 2015

Innehåll

1. Sammanfattande analys

Tidigare granskningar har visat att landstinget saknat landstingsövergripande system för att ta fram förteckningar över vilka behörigheter olika medarbetare har till IT-system.

Denna granskning visar att landstingsstyrelsen och hälso- och sjukvårdsnämnden inte säkerställt en tillräcklig kontroll av personalens behörigheter till journalsystemet SYSteam Cross. Av fyra kontrollerade basenheter saknade samtliga dokumenterade rutiner för beställning, tilldelning, ändring och borttagning av behörigheter till såväl journalsystemet som till övriga IT-system.

Vi har kontrollerat behörigheter till journalsystemet för samtliga tjänster i landstinget som avslutats under september, oktober och november 2015. Totalt rör det sig om 311 tjänster som avslutats. Av dessa hade 223 personer anställningar där de haft behörighet till journalsystemet. Vår kontroll visade att 79 personer fortfarande hade behörighet till journalsystemet trots att tjänsten var avslutad enligt landstingets lönesystem. En fördjupad kontroll vid fyra basenheter visade att det i vissa fall fanns orsaker till att personer fortfarande hade kvar sina behörigheter. I ca 70 procent av fallen hade verksamhetscheferna dock missat att säkerställa att behörigheterna blivit avslutade.

1.1. Rekommendationer

Vi rekommenderar landstingsstyrelsen och hälso- och sjukvårdsnämnden att säkerställa att:

- verksamheterna har dokumenterade rutiner för administration av behörighter till IT-system.
- Verksamheterna genomför regelbundna kontroller av de anställdas IT-behörigheter.
- Personer som inte ska ha tillgång till journalsystemet inte har behörighet till systemet.

2. Bakgrund

Medarbetare i landstinget har behörighet till flera olika IT-system. Tidigare granskningar visar att det på landstingsövergripande nivå inte finns något system för att ta fram förteckningar över vilka behörigheter olika medarbetare har till landstingets IT-system (15/2014, 22/2014) .

Enligt landstingsdirektörens riktlinjer, *Informationssäkerhet – riktlinjer för åtkomst till elektronisk information*, ansvarar respektive verksamhetschef för att dess personal har rätt behörigheter. Personalens behörigheter ska begränsas till vad som är nödvändigt för att ge en god och säker vård.

Våra stickprov av följsamhet till administrativa rutiner har tidigare visat att personer som avslutat sin anställning fortfarande har behörighet till journalsystemet SYSteam Cross (Rapport nr 22/2014).

2.1. Revisionsfrågor

Den övergripande revisionsfrågan som granskningen avsett att besvara var om landstingsstyrelsen säkerställt en ändamålsenlig kontroll av medarbetarnas behörigheter till IT-system?

För att besvara den övergripande revisionsfrågan har vi använt oss av underliggande revisionsfrågor. Har ansvarig styrelse eller nämnd säkerställt att:

- Det finns dokumenterade riktlinjer för tilldelning, ändring och borttagning av behörigheter till IT-system?
- Det finns dokumenterade rutiner för kontroll av personalens behörigheter?
- Regelbundna kontroller av behörigheter till IT-system genomförs?
- Det inte finns det felaktigt registrerade behörigheter till journalsystemet SYSteam Cross?

2.2. Avgränsning

Granskningen är avgränsad till att kontrollera behörighet till journalsystemet SYSteam Cross.

2.3. Metod

Granskningen har bestått av dokumentstudier och intervjuer med systemägare för SYSteam Cross, fyra verksamhetschefer och fyra lokalt informatiksystemansvariga (LISA). Vi har även genomfört ett stickprov för att kontrollera om det finns felaktigt registrerade behörigheter.

2.4. Revisionskriterier

Med revisionskriterier avses de bedömningsgrunder som bildar underlag för revisionens analyser, slutsatser och bedömningar. Vi har utgått från följande revisionskriterier:

- Kommunallagen 6 kap. 7§.
- Landstingsfullmäktiges reglemente för landstingsstyrelsen.
- Patientdatalagen (2008:355), kap 4, kap 6.
- Socialstyrelsens föreskrifter (SOSFS 2008:14), kap 2

3. Patientdatalagen

Enligt 2 kap. 2 § patientdatalagen ska vårdgivaren bestämma tilldelning av behörighet till sådana uppgifter om patienter som förs helt eller delvis automatiserat. Behörigheterna ska begränsas till vad som är nödvändigt för att den enskilde ska kunna fullgöra sina arbetsuppgifter.

4. Socialstyrelsens föreskrifter

Av 2 kap. 6 § i SOSFS 2008:14 framgår att vårdgivaren ansvarar för att det i ledningssystemet finns rutiner som säkerställer att personalens behörighet begränsas till vad som är nödvändigt för att ge en god och säker vård. Av föreskriften framgår också att vårdgivaren ansvarar för att det finns rutiner för tilldelning, förändring, borttagning och uppföljning av behörigheter.

Enligt 2 kap. 19 § SOSFS 2008:14 ansvarar verksamhetschefen att utdelade behörigheter till åtkomst till patientuppgifter är ändamålsenliga och förenliga med personalens aktuella arbetsuppgifter.

5. Riktlinjer för hantering av IT-behörigheter

Enligt de riktlinjer som lanstingsdirektören fastställt framgår att verksamhetschefen ansvarar för att personalen har rätt behörighet. Personalens behörighet ska begränsas till vad som är nödvändigt för att ge en god och säker vård. Av riktlinjerna framgår att verksamheterna ska ha dokumenterade rutiner för beställning, tilldelning, ändring och borttagning av behörigheter.

Av riktlinjerna framgår att verksamhetschefen ansvarar för att personalen har rätt behörighet. Verksamheterna ska genomföra regelbundna kontroller av användarnas behov av behörigheter.

6. SYSteam Cross

För journalföring använder Västerbottens läns landsting IT-systemet SYSteam Cross. För att en användare ska kunna logga in i systemet krävs, förutom en giltig behörighet, ett SITHS-kort och kopplade medarbetaruppdrag. Verksamheterna beställer behörigheter via webfacit som är ett beställningssystem i landstinget.

7. Följsamhet till riktlinjer

Vi har kontrollerat om fyra basenheter har dokumenterade riktlinjer för beställning, tilldelning, ändring och borttagning av behörigheter. De fyra basenheter vi kontrollerat är:

- Akutsjukvården
- Barn- och ungdomsklinik
- Burträsk hälsocentral
- Kirurgcentrum

Akutsjukvården har inte några dokumenterade rutiner för tilldelning, ändring och borttagning av behörigheter. En person på basenheten ansvarar för att administrera behörigheterna till SYSTeam Cross.

Barn- och ungdomskliniken har, enligt verksamhetschefen, en skriftlig rutin där det framgår att avdelningschef kontaktar datasamordnare eller chefsassistent vid förändringar av anställdas behörigheter. Med anledning av av vår granskning har basenheten under arbetet förändrat sina rutiner. Den nya rutinen innebär att basenhetens HR-specialist vid avslut av anställningar ska meddela datasamordnare eller chefassistent att lägga in ärende i webfacit.

Verksamhetschefen på Burträsk Hälsocentral har uppgett att basenheten inte har några formella skriftliga rutiner utan att basenhetens LISA följer de anvisningar hon har i sitt uppdrag.

En av kirurgcentrums lokalt systemansvariga har uppgett att basenheten har skriftliga mallar för vilka systembehörigheter som ska beställas till respektive yrkeskategori. Basenheten saknar i övrigt skriftliga rutiner för tilldelning, ändring och borttagning av behörigheter till IT-system. De lokalt systemansvariga som handlägger behörigheter till IT-system har uppgett att de agerar utifrån beslut från respektive chef.

7.1. Stickprov avslutade behörigheter

Vi har kontrollerat om samtliga personer som avslutade sina anställningar vid landstinget under månaderna september till november 2015 har fått sina behörigheter till journalsystemet SYSteam Cross avslutade. Totalt har under denna period 311 personer avslutat sin anställning vid landstinget. Av dessa hade 223 personer anställningar där de haft behörighet till SYSteam Cross. Resultatet av kontrollen var följande:

Status	**Antal personer**
Avslutad behörighet	86
Ej avslutad behörighet men annan anställning inom VLL	28
Ej avslutad behörighet, men användaren kan inte logga in i SYSteam Cross	30
Ej avslutad behörighet	79
Summa	**223**

Vi har genomfört en fördjupad kontroll vid fyra basenheter. Den person som administrerar behörigheterna vid basenheten akutsjukvård Umeå har uppgett att en av dessa personer fortfarande arbetar som timanställd vid basenheten. Vår kontroll visade att 8 personer vid kirurgcentrum som enligt lönesystemet avslutat sin anställning fortfarande hade behörighet till SYSteam cross. Enligt verksamhetschefen ska 4 av dessa ha behörighet då de fortfarande arbetar som timanställda vid basenheten. Verksamhetscheferna vid barn- och ungdomskliniken och Burträsk hälsocentral bekräftar att man inte avslutat behörigheterna.

Av sammanställningen nedan framgår utfallet vid den utökade kontrollen.

Basenhet	**Behörighet trots att anställning upphört enligt lönesystemet**	**Arbetar som timanställd enligt verksamhetschef**	**Saknar förklaring varför behörighet kvarstår trots att anställningen är avslutad**
Akutsjukvård Umeå	3	1	2
Barn- och ungdomsklinik	6	0	6
Burträsk hälsocentral	2	0	2
Kirurgcentrum	8	4	4
Totalt	**19**	**5**	**14**

Enligt verksamhetschefernas uppgifter ska alltså 5 av de 19 kontrollerade personerna ha fortsatta behörigheter. 14 av de 19 kontrollerade personerna borde inte ha haft sina behörigheter kvar. Det motsvarar cirka 70 procent av det totala antalet kontrollerade personer.

8. Svar på revisionsfrågor

Ingen av de fyra basenheter som vi kontrollerat hade skriftliga rutiner för tilldelning, förändring och avslut av IT-behörigheter. Ingen av basenheterna hade genomfört några kontroller av personalens behörighet till SYSteam Cross.

Vår kontroll visar att 79 personer som enligt lönesystemet avslutat sin anställning fortfarande hade behörighet till journalsystemet SYSteam Cross. Våra fördjupade kontroller vid fyra basenheter visade att det i vissa fall fanns förklaringar till att personer fortfarande hade kvar sina behörigheter. Vårt stickprov visade dock att i mer än 70 procent av fallen har basenheterna ej avslutat behörigheten för personal som inte längre ska ha behörighet till journalsystemet.

Vi bedömer att landstingsstyrelsen och hälso- och sjukvårdsnämnden inte har säkerställt en ändamålsenlig kontroll av att medarbetarnas behörigheter till IT-system. Nedan ger vi svar på våra underliggande revisonsfrågor:

Revisionsfråga	Svar
Finns dokumenterade rutiner för kontroll av personalens behörigheter?	Nej. De basenheter vi har kontrollerat saknar dokumenterade rutiner.
Genomförs regelbundna kontroller av behörigheter till IT-system?	Nej.
Är registrerade behörigheter till SYSTeam Cross korrekta?	Nej. En kontroll av samtliga personer som avslutat sin anställning under perioden september till november 2015 visade att 79 personer fortfarande hade behörighet till SYSteam Cross. Fördjupade kontroller visade att 70 procent inte skulle ha behörighet.

9. Rekommendationer

Vi rekommenderar landstingsstyrelsen, hälso- och sjukvårdsnämnden och nämnden för funktionshinder och habilitering att säkerställa att:

- verksamheterna har dokumenterade rutiner för administration av behörighter till IT-system.
- Verksamheterna genomför regelbundna kontroller av de anställdas IT-behörigheter.
- Personer som inte ska ha tillgång till journalsystemet inte har behörighet till systemet.

Umeå den 25 februari 2016

Jonas Hansson
revisor
Västerbottens läns landsting