Ragunda Kommun

Revisorerna

2017-~~11-23~~ · 12 · 14

Kommunstyrelsen
För kännedom: Kommunfullmäktiges presidium

Revisionsrapport "Rutiner för behörigheter IT-system inom äldreomsorg"

Revisionen har via KPMG genomfört en granskning av rutiner för behörigheter till IT-system inom äldreomsorgsverksamheten.

Revisionen hemställer om att kommunstyrelsen lämnar synpunkter avseende de rekommendationer och förslag som lyfts fram i rapportens sammanfattning.

Revisionen emotser svar senast den 28 februari 2018.

För Ragunda kommuns revisorer

Vidar Lind
Ordförande

Maud Lindström
Vice ordförande

Rutiner för behörigheter IT-system inom äldreomsorg

Vid revisionens möte den 30 mars 2017 fick KPMG i uppdrag att undersöka rutiner för behörigheter till IT-system inom äldreomsorg.

1. Syfte

Syftet med granskningen är att bedöma om det finns en ändamålsenlig styrning avseende behörigheter.

Vi har därför granskat

om det finns styrdokument som hanterar behörighetstilldelning

om uppföljning av behörighetsstyrning genomförs

2. Revisionskriterier

Vi har bedömt om rutinerna/verksamheten uppfyller

- HSLF-FS 2016:40

3. Metod

Granskningen har genomförts genom dokumentgranskning och intervju med förvaltningschef, systemansvarig och IT-samordnare.

4. HSLF-FS 2016:40

Enligt Socialstyrelsens föreskrift HSLF-FS 2016:40 Journalföring och behandling av personuppgifter i hälso- och sjukvården ställs krav på vårdgivaren avseende bl.a. behörigheter. Det övergripande syftet är att säkerställa personuppgifternas tillgänglighet, riktighet, konfidentialitet och spårbarhet.

- Tillgänglighet – patientuppgifter i vårdgivarens dokumentation är åtkomlig och användbar för den som är behörig
- Riktighet – patientuppgifterna är oförvanskade
- Konfidentialitet – obehöriga ska inte kunna ta del av patientuppgifterna

- Spårbarhet – det går att härleda åtgärder till en identifierad användare

Det innebär bland annat att vårdgivarens ska bestämma villkoren för tilldelning av behörighet för åtkomst till uppgifter om patienter. Behörigheten ska begränsas till vad som behövs för att den enskilde ska kunna fullgöra sina arbetsuppgifter. Vårdgivaren ansvarar för att alla användare har en individuell behörighet vilket innebär att endast personliga inloggningar är tillåtna. 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.

4.1 Nuläge och bedömning

Granskningen har varit inriktad på verksamhetssystemet Treserva utifrån att det har flest användare.

Tilldelning av behörigheter sker genom beställning av medarbetarens närmaste chef. Blanketten *Ansökan om behörighet – Treserva* fylls i där verksamhetsroll samt omfattning av dataåtkomst på enhetsnivå regleras (ex Utförare ÄO SoL – Bispgården ordinärt boende). Blanketten skickas till IT-samordnare som tilldelar behörighet i systemet, och sparar blanketten i särskild pärm. Det finns även möjlighet att reglera omfattning av dataåtkomst på avdelningsnivå. Blanketten ska även användas vid förändring av behörigheter, t ex när en medarbetare byter arbetsplats. Rutin för tilldelning eller förändring av behörigheter finns inte dokumenterad.

Efter inloggning i kommunens system, sker ytterligare en inloggning till Treserva av medarbetaren. I samband med introduktionen får medarbetaren en genomgång av IT-samordnare eller administratör gällande teknik och informationssäkerhet. I övrigt svarar verksamheten för att medarbetarna har erforderliga kunskaper, t ex gällande dokumentation. Ett exempel som flertalet kommuner nyttjar för utbildning av användare i kommunens IT-miljö är DISA, en informationssäkerhetsutbildning via webb som tillhandahålls kostnadsfritt av Myndigheten för samhällsskydd och beredskap.

För närvarande pågår en genomgång av befintliga behörigheter i Treserva mot personalsystemet, för att ta bort behörigheter för personer som inte längre är anställda. Dokumenterade rutiner eller upparbetat arbetssätt för borttagning och regelbunden uppföljning av behörigheter saknas.

Utifrån nuläget kan vi konstatera att de krav som ställs i HSLF-FS 2016:40 inte uppfylls. Utöver kraven ovan finns även ytterligare krav på vårdgivaren, bl.a. gällande informationssäkerhetspolicy och dokumenterade riskanalyser. Då föreskriften gäller sedan mars 2017 finns anledning för kommunstyrelsen att säkerställa att resurser avsätts för att uppfylla kraven.

I sammanhanget bör noteras att det för närvarande pågår ett utvecklingsarbete med utgångspunkt i de nya regler gällande informationssäkerhet som träder i kraft under våren 2018.

Vi rekommenderar kommunstyrelsen att fastställa en tidplan och resurssatt åtgärdsplan, som följs upp löpande och att eventuella avvikelser då hanteras.

KPMG AB, dag som ovan

Mikael Lindberg
Kommunal revisor