2019-07-05

Omvårdnadsnämnden i Gävle kommun

Granskning av behörighetsstyrning i verksamhetssystemet Treserva ur ett dataskyddsrättsligt perspektiv

Dataskyddsombudet har genomfört en granskning av omvårdnadsnämndens verksamhetssystem Treserva. Granskningen har fokuserat på hur nämnden sköter behörighetsstyrningen i systemet ur ett dataskyddsrättsligt perspektiv.

Granskningen har genomförts genom en intervju (190515) där systemförvaltningspersonal och dataskyddssamordnare deltagit. Dessutom har verksamheten kompletterat med skriftligt underlag.

Rättsliga utgångspunkter

Allmänna krav som gäller för hela socialnämndens verksamhet

Dataskyddsförordningens art. 5 reglerar ett antal grundläggande principer som varje personuppgiftsansvarig organisation ska följa i all personuppgiftsbehandling.

Tekniska och organisatoriska åtgärder för att skydda informationen, kontrollera den och säkerställa en lämplig säkerhetsnivå

En av de grundläggande principerna uttrycker att man alltid måste värna om de registrerades integritet och uppgifternas konfidentialitet när man behandlar personuppgifter, det vill säga säkerställa att de skyddas genom att hitta lämpliga tekniska och organisatoriska säkerhetsåtgärder. Det kan dels handla om att förhindra intrång och att obehöriga får tillgång till uppgifter, men även om att säkerställa att uppgifterna inte skadas eller raderas av misstag. En av åtgärderna kan exempelvis vara att både tekniskt och organisatorisk styra och kontrollera vilka personer som har åtkomst till vilken information.

Utöver de grundläggande principerna reglerar även art. 24 att den personuppgiftsansvarige ska vidta lämpliga tekniska eller organisatoriska åtgärder för att kunna visa att behandlingen utförs i enlighet med förordningen. Åtgärderna ska ses över och uppdateras vid behov.

Vidare ska den personuppgiftsansvariga vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämpligt i förhållande till risken (art. 32). I beaktande ska bland annat tas den senaste

utvecklingen, genomförandekostnaderna, behandlingens art, omfattning, sammanhang och ändamål samt riskerna av varierande sannolikhetsgrad och allvar.

Skyldighet att visa hur de grundläggande principerna efterlevs

Enligt ansvarsprincipen (art. 5.2) ska den personuppgiftsansvariga även kunna visa att de grundläggande principerna för personuppgiftsbehandling efterlevs. Detta kan exempelvis ske genom att ta fram rutiner, instruktioner och riktlinjer, utbilda personal, bygga in integritetsvänliga lösningar i systemen och föra register över behandlingar.

En relevant del av dokumentationen kan exempelvis vara

- en dokumenterad och beslutad systemförvaltningsorganisation med tydliga roller och ansvar,
- riktlinjer och rutiner för behörighetsstyrning,
- riktlinjer och roller för loggkontroller,
- dokumentation av hur bedömningarna i samband med behörighetsstyrning har gjorts,
- hur konstaterade avvikelser vid genomförda loggkontroller har hanterats och åtgärdats.

Krav som gäller specifikt inom hälso- och sjukvården

Dataskyddsförordningen ställer grundläggande krav på all personuppgiftsbehandling. Inom verksamheter där hälso- och sjukvårdslagen gäller, ställs ytterligare och striktare krav på behandling av patientuppgifter och informationssäkerhet. Dessa krav regleras i patientdatalagen men även i Socialstyrelsens föreskrift (HSLF-FS 2016:40) om journalföring och behandling av personuppgifter i hälso- och sjukvården. Därutöver finns råd av mer praktisk och konkret karaktär i handboken Journalföring och behandling av personuppgifter inom hälso- och sjukvården. Även Datainspektionen har lämnat råd avseende hanteringen av patientuppgifter på sin hemsida[1] och ställningstaganden genom äldre tillsynsärenden.

Patientdatalagens krav avseende behörighetsstyrning och loggkontroll

Personuppgifter ska enligt patientdatalagen utformas och i övrigt behandlas så att patienters och övriga registrerades integritet respekteras. Personuppgifter ska hanteras och förvaras så att obehöriga inte får tillgång till dem. (1 kap. 2 § PDL) Den som arbetar hos en vårdgivare får ta del av dokumenterade uppgifter om en patient endast om han eller hon deltar i vården av patienten eller av annat skäl behöver uppgifterna för sitt arbete inom hälso- och sjukvården. (4 kap. 1 § PDL)

[1] https://www.datainspektionen.se/lagar--regler/patientdatalagen/hur-forhindrar-man-obefogad-spridning-av-patientuppgifter/

Vidare ska en vårdgivare bestämma villkor för tilldelning av behörighet för åtkomst till sådana uppgifter om patienter som förs helt eller delvis automatiserat. Sådan behörighet ska begränsas till vad som behövs för att den enskilde ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården. (4 kap. 2 § PDL) En vårdgivare ska även se till att åtkomst till sådana uppgifter om patienter som förs helt eller delvis automatiserat dokumenteras och kan kontrolleras. Vårdgivare ska göra systematiska och återkommande kontroller av om någon obehörigen kommer åt sådana uppgifter. (4 kap. 3 § PDL)

Krav på behörighetsstyrning och loggkontroll enligt Socialstyrelsens föreskrift om journalföring och behandling av personuppgifter i hälso- och sjukvården (HSLF-FS 2016:40)

Vårdgivaren ska ansvara för att det finns en informationssäkerhetspolicy. Den ska ange vårdgivarens övergripande mål för och inriktning på verksamhetens arbete med informationssäkerhet i syfte att säkerställa personuppgifters tillgänglighet, riktighet, konfidentialitet och spårbarhet. (3 kap. 4 §)

Vårdgivaren ska årligen utvärdera skyddet mot såväl intern som extern olovlig åtkomst till datornätverk och informationssystem som används för behandling av personuppgifter. (3 kap. 18 §)

Vårdgivaren ska ansvara för att varje användare tilldelas en individuell behörighet för åtkomst till personuppgifter. Vårdgivarens beslut om tilldelning av behörighet ska föregås av en behovs- och riskanalys. (4 kap. 2 §)

Vårdgivaren ska ta fram rutiner för ändring, borttagning och regelbunden uppföljning av behörigheterna för att säkerställa att dessa är riktiga och aktuella. (4 kap. 3 §)

Vårdgivaren ska ansvara för att

1. det av dokumentationen av åtkomsten (loggar) framgår vilka åtgärder som har vidtagits med uppgifter om en patient,
2. det av loggarna framgår vid vilken vårdenhet eller vårdprocess åtgärderna vidtagits,
3. det av loggarna framgår vid vilken tidpunkt åtgärderna vidtagits,
4. användarens och patientens identitet framgår av loggarna,
5. systematiska och återkommande stickprovskontroller av loggarna görs,
6. kontroller av loggarna dokumenteras, och
7. loggarna sparas minst fem år för att möjliggöra kontroll av åtkomsten till uppgifter om en patient. (4 kap. 9 §)

Särskilt om individuell behörighetstilldelning

Kravet på individuell behörighetstilldelning innebär bland annat att alla användare har en individuell behörighet och att endast individuella inloggningar är tillåtna. En vårdgivare ska begränsa en användares behörigheter till vad som behövs för att användaren ska kunna fullgöra sina arbetsuppgifter inom hälso-

och sjukvården och till vad som är nödvändigt för att ge en god och säker vård. Behovs- och riskanalyser har en avgörande betydelse för en väl avvägd behörighetstilldelning. Om en vårdgivare inte har genomfört dessa analyser före tilldelningen av behörigheter, riskerar vårdgivaren att ha en alltför vidsträckt och grovmaskig eller till och med felaktig behörighetstilldelning, vilket leder till en obefogad spridning av patientuppgifter. Behovsanalysen ska komma fram till vilken information olika personkategorier och olika slags verksamheter behöver. Riskanalysen ska ta hänsyn till olika slags risker som kan vara förknippade med alltför vid tillgänglighet avseende vissa slags uppgifter. Ju mer omfattande ett system är, desto större mängd olika behörighetsnivåer måste det finnas. [2]

Det är inte tillräckligt att vårdgivaren nöjer sig med att i allmänna ordalag uttrycka, exempelvis i olika policydokument, att behovs- och riskanalyser ska genomföras. Vårdgivaren behöver besluta om en behovs- och riskanalys utifrån patientuppgifterna i informationssystemet som sådant och inte enbart nöja sig med att utgå ifrån vilken yrkeskategori en viss befattningshavare tillhör eller att alla med viss typ av legitimation ska ha en och samma behörighetsprofil i systemet. Att en vårdgivare exempelvis utbildar personalen om när de får ta del av patientuppgifter enligt den inre sekretessen, ger personalen instruktioner i form av policydokument, riktlinjer eller annat informationsmaterial eller informerar om och genomför loggkontroller, innebär *inte att vårdgivaren kan förbise kraven på att behörighetstilldelning ska föregås av en reell behovs- och riskanalys*. [3]

Datainspektionens råd om överväganden i en behovs- och riskanalys

Datainspektionen rekommenderar att man i en behovs- och riskanalys tydliggör och konkretiserar befattningshavares olika uppdrag till omfattning och innehåll utifrån yrkeskategori, specifika uppdrag, arbetssätt och arbetsställe samt faktiska arbetsuppgifter. Därefter ska man fastställa behovet av åtkomst till patientuppgifter hos olika slags verksamheter utifrån arbetssätt, omfattning och uppdrag och bedöma om det förekommer särskilt skyddsvärda patientuppgifter eller patientgrupper, exempelvis personer med skyddad identitet, eller särskilt vårdbehov/diagnos.

Dessa överväganden behöver vårdgivaren också genomföra beträffande alla anställda som får del av patientuppgifter, det vill säga även de som arbetar med verksamhetsuppföljning, statistikframställning, central ekonomiadministration, teknisk drift eller andra arbetsuppgifter som inte primärt rör vården av patienter.[4]

---

[2] Socialstyrelsens handbok Journalföring och behandling av personuppgifter inom hälso- och sjukvården
[3] https://www.datainspektionen.se/lagar--regler/patientdatalagen/hur-forhindrar-man-obefogad-spridning-av-patientuppgifter/
[4] https://www.datainspektionen.se/lagar--regler/patientdatalagen/hur-forhindrar-man-obefogad-spridning-av-patientuppgifter/

Datainspektionens råd avseende loggkontroller

Det är nödvändigt att kontrollerna genomförs regelbundet och omfattar en så hög andel av logghändelserna att det blir en effektiv kontroll. Hur ofta loggkontroller genomförs beror på verksamhetens omfattning, antalet personer med åtkomst, hur behörigheterna delas ut och hur omfattande kontrollerna är. Personalen ska vara informerade om att loggkontroller sker.

Loggkontroller är inte verkningsfulla om inte vårdgivaren gett riktlinjer till de befattningshavare som gör bedömningar i samband med loggkontrollerna om vad som kan utgöra obehörig elektronisk åtkomst enligt reglerna om inre sekretess. Om sådana riktlinjer saknas riskerar vårdgivaren att åsidosätta den inre sekretessen.[5] Datainspektionen har tagit fram en checklista som stöd för vårdgivarnas arbete med systematiska logguppföljning. [6]

Behörighetsstyrning och loggkontroll i Treserva, omvårdnadsnämnden i Gävle kommun

Systemförvaltningsorganisation

Omvårdnadsnämndens förvaltningsorganisation för Treserva består av objektägare, systemförvaltningsledare, systemförvaltare och systemadministratörer. Det finns en framtagen systemförvaltningsplan men den är inte specifikt anpassad för Treserva.

Systemförvaltningsorganisationens uppgifter, ansvar och mandat har inte dokumenterats.

Behörighetsstyrning

Behörigheterna för Treserva styrs utifrån vilket regelverk som gäller för viss verksamhet men även vilken funktion och befattning en anställd har och vilken verksamhet han/hon arbetar inom.

Respektive chef beställer behörigheter till nyanställda utifrån olika behörighetspaket. Det är vanligt förekommande att en användare behöver ha ”bra att ha” behörigheter för att kunna arbeta flexibelt i en viss verksamhet. Inom nämndens verksamheter tillämpas även en centralt framtagen, övergripande checklista som gäller för behörighetsbeställning vid nyanställning.

Det finns en teknisk lathund för enhetschefer som stöd för att ta bort tilldelade behörigheter som inte längre är aktuella. Det finns även en övergripande rutin

---

[5] https://www.datainspektionen.se/lagar--regler/patientdatalagen/hur-forhindrar-man-obefogad-spridning-av-patientuppgifter/
https://www.datainspektionen.se/lagar--regler/patientdatalagen/systematisk-logguppfoljning/

[6] https://www.datainspektionen.se/lagar--regler/patientdatalagen/systematisk-logguppfoljning/

i Gävle kommun där anmälan ska göras när en anställd slutar i sin tjänst; för att kunna ta bort tillgång till olika system.

Systemförvaltare ansvarar för att se över behörigheten för roller/professioner utifrån nya eller förändrade behov. Utifrån den nya organisationen kommer en översyn av befintliga roller/ansvar/befogenheter ses över. Detta ska vara genomfört senast årsskiftet.

Behörighetsstyrningen är inte anpassad efter de krav som gäller för hälso- och sjukvården.

Loggkontroll

Det finns rutiner för loggkontroll för Treserva, men rutinerna är bristfälliga och har inte dokumenterats. Rutinerna är inte anpassade efter de krav som gäller för hälso- och sjukvården.

Funktionerna för loggkontroll i Treserva är bristfälliga och kontroller kan för närvarande endast genomföras på beställning då chefer specificerar vilken användare som avses. För närvarande går det inte att genomföra slumpmässiga urval för loggkontroll. Diskussion har förts med leverantören under en längre period; problemet borde ha varit löst i början av året.

Rutinen för loggkontroll följs därmed i låg omfattning. Det kan ske kontroller vid misstanke men några kontinuerliga systematiska kontroller genomförs inte.

Dataskyddsombudets bedömning

Ju känsligare information som behandlas, desto större tydlighet krävs för systemförvaltningsorganisationen (vem gör vad i systemet, vem ansvarar för vad), hur den enstaka anställdes behörighet och tillgång till information i systemet styrs och hur felaktigheter och oegentligheter kontrolleras (varför, hur, vad, när och vem).

Dokumentationen av hur den personuppgiftsansvariga organisationen resonerar, bedömer, kontrollerar och verkställer sitt informationssäkerhetsarbete kring ett verksamhetssystem där stora mängder känslig information om människor behandlas, är av stor betydelse för uppfyllandet av ansvarsprincipen (art. 5) och de övriga kraven som redovisats ovan.

Omvårdnadsnämnden har en odokumenterad systemförvaltningsorganisation för Treserva och en generell systemförvaltningsplan. Av dessa framgår inte vad de olika rollerna i organisationen förväntas och får göra i systemet Treserva.

Nämnden har vissa rutiner för behörighetsstyrningen men dessa är endast delvis dokumenterade. Rutinerna uppfyller inte kraven som gäller för hälso- och sjukvården.

Nämnden har vissa rutiner för loggkontroll, men rutinerna är bristfälliga och dokumenterade endast delvis. Rutinerna uppfyller inte kraven som gäller för hälso- och sjukvården. Några systematiska loggkontroller genomförs inte.

Dataskyddsombudet bedömer att omvårdnadsnämnden brister i sitt arbete med behörighetsstyrning och loggkontroll. Om nämnden inte vidtar åtgärder riskerar den skyddet av personuppgifterna vilket drabbar de registrerades rättigheter och friheter. Att inte följa dataskyddsförordningens krav kan, förutom skadat anseende, även leda till omfattande sanktionsavgifter vid en eventuell tillsyn genomförd av Datainspektionen (art. 83).

Dataskyddsombudets rekommendation

Dataskyddsombudet rekommenderar att omvårdsnämnden

- dokumenterar sin systemförvaltningsorganisation för systemet Treserva,
- dokumenterar och kompletterar rutiner för behörighetsstyrning och säkerställer att rutinen, för den delen den tillämpas inom hälso- och sjukvården, följer kraven som gäller för hälso- och sjukvården,
- i samråd med leverantören säkerställer att det blir tekniskt möjligt att arbeta med systematiska loggkontroller,
- dokumenterar och kompletterar rutiner för loggkontroller och säkerställer att rutinen, för den delen den tillämpas inom hälso- och sjukvården, följer kraven som gäller för hälso- och sjukvården.

I tjänsten,

Anu Sundin
Dataskyddsombud
Gävle kommuns dataskyddsenhet