

4.5 Riktlinje för loggkontroll enligt informationshantering och journalföring i hälso- och sjukvårdsdokumentation

Denna riktlinje är ett komplement till Tyresö kommuns IT-säkerhetspolicy och Informations-säkerhetspolicy och riktar sig till verksamhetschefer och personer som ges ett delegerat ansvar för loggkontroll i vårdinformation (dokumentationssystem) till systemägare. Riktlinjen kan behöva kompletteras via aktuell systemägare med mer specifika rutinbeskrivningar beroende på hur respektive systems loggfunktion är utformad.

Syfte

Syftet med loggkontroll är att granska att tillgång till uppgifter angående patienter/boende på vård- och omsorgsboende nyttjas enligt gällande regelverk. Kontrollen ska ske på ett systematiskt och regelbundet sätt.

Medarbetare som tilldelas behörighet till vårdinformation ges en teknisk möjlighet att ta del av information angående patienter/boende. Detta innebär att möjligheten föreligger att ta del av informationen i omvårdnadsjournalen för den medarbetare som är inbegripen i vården. De medarbetare som inte är inbegripen i vård och behandling har inte rätt att ta del av denna information.

Behörigheten till systemet styrs via användaridentiteten och användarens personliga lösenord alternativt via eTjänstekort (SITHS-kort). Detta möjliggör spårbarhet i systemet genom loggning. Förutom att loggen kan användas som underlag vid utredning av felaktig eller obehörig användning så utgör den också en säkerhet för användarna mot ogrundade misstankar.

Kunskap om att loggning och loggkontroller sker har en förebyggande inverkan och avskräcker från obehörig åtkomst. Detta förutsätter att användarna informeras om den loggning och loggkontroll som utförs.

Loggkontroll får inte användas till arbets- och prestationsmätning eller på ett sådant sätt att det kan medföra risk för intrång i medarbetarens personliga integritet.

Ansvar

Verksamhetschefen har det övergripande ansvaret för hantering av omvårdnadsjournaler inom sitt verksamhetsområde. Behörigheter i dokumentationssystemet måste stämma överens med antalet anställda inom verksamheten. Verksamhetschefen ska löpande se till att medarbetarna fullföljer de uppdrag som följer av anställningen, på ett sätt som överensstämmer med lagstiftning, föreskrifter, etiska riktlinjer eller som följer av yrket.

Medicinskt ansvarig sjuksköterska ansvarar för

- att det finns riktlinjer för loggkontroll för informationshantering och journalföring i hälso- och sjukvårdsdokumentationen
- att följa upp loggkontrollerna vid kvalitetstillsyn, enligt Systematiskt kvalitetsledningssystem SOSFS 2011:9.

Systemägare ansvarar för

- att behörigheter läggs in i dokumentationssystemet för legitimerad och behörig personal
- att med stöd av verksamhetschef granska att tillgång till uppgifter angående patienter/boende på vård- och omsorgsboendet används enligt gällande regelverk
- att tillsammans med verksamhetschef utföra loggkontroll.

Verksamhetschefen ansvarar för

- att det finns en **lokal rutin för systematisk stickprovskontroll** i hälso- och sjukvårdsdokumentationen
- att det i den lokala rutinen framgår vem som ansvarar för att informera systemägare när personal nyanställs eller slutar sin anställning (detta för att systemägare ska kunna tilldela, förändra och avsluta behörigheter för verksamhetens personal)
- att behörigheterna är ändamålsenliga och förenliga med aktuella arbetsuppgifter
- att tillsammans med systemägare via loggkontroll följa upp och kontrollera att användare följer de regler och rutiner som gäller för åtkomst till uppgifter angående patienter/boende
- att varje användare informeras om att loggning och loggkontroll utförs, samt konsekvenser vid överträdelse
- att personalen är informerade om gällande lagstiftning och bestämmelser som gäller för hantering av uppgifter/information om patienter/boende i dokumentationssystemet.
- att det i introduktionen för nyanställda ingår att loggningar i dokumentationssystemet sker systematiskt
- initiera loggkontroll vid misstanke om obehörig åtkomst till vårddokumentation (punkt 3 i kontrollrutiner) samt andra riktade loggkontroller (punkt 4 i loggkontroll)

Användaren ansvarar för

- att ta del av och vara uppdaterad om rutiner och regler och att följa dessa
- att rapportera till närmaste chef om brister i rutiner eller om oegentligheter upptäcks
- att kontrollera att rätt behörighet har tilldelats
- att personliga lösenord inte kan bli tillgängliga för obehöriga
- att datorer och annat informationsmaterial, såsom telefoner eller USB-minnen som har använts inte lämnas utan att uppgifterna angående patienten/boende är skyddade från obehörig åtkomst
- att endast ta del av uppgifter angående patienten/boende om man deltar i vården av den berörda eller av något annat ändamål som anges i gällande regelverk då man behöver uppgifterna för sitt arbete.

Kontrollrutiner**1. Systematisk stickprovskontroll**

Varje månad ska ett antal användare (10 %) inom verksamheten slumpmässigt väljas ut, vars loggar granskas under en 24-timmarsperiod.

Antalet användare som kontrolleras varje månad bör omfatta så många att det motsvarar sannolikheten att varje användare blir granskad minst en gång per år.

Av loggarna ska det framgå:

- om vårddokumentation har öppnats
- om vårddokumentation har upprättats
- om vårddokumentation har skrivits ut
- vid vilken vårdenhet och vid vilken tidpunkt åtgärderna har vidtagits
- användarens och patientens identitet

Loggarna checkas av mot anteckningarna i journalen. Dessa loggkontroller ska sparas i minst 10 år.

2. Vid patient/boendes begäran om loggutdrag

En patient/boende kan begära ett loggutdrag över vilka som haft tillgång till dennes journal. I samband med att loggutdraget skickas till patient/boende ska loggkontroll göras för den tidsperiod som angivits av patient/boende. I loggen syns vilken enhet, roll och tidpunkt någon tagit del av journalen.

Den information om loggarna som ska lämnas ut ska vara anpassad till och klagörande för patient/boende och det ska framgå från vilken verksamhet och vid vilken tidpunkt någon har tagit del av uppgifterna. Dokumenteras i omvårdnadsjournalen.

3. Kontroll vid misstanke om obehörig åtkomst till vårdinformation

Vid misstanke om obehörig åtkomst till vårdinformation ska loggkontroll ske omedelbart.

Är misstanken riktad mot en specifik användare ska kontrollen ske för den tidsperiod som misstanken omfattar.

Det kan även finnas skäl att granska loggen för en viss patient/boende om det rör sig om en offentlig person eller att det finns en patient/boende som är involverad i en händelse som kan bli massmedialt uppmärksammas.

4. Andra riktade loggkontroller

Särskild kontroll ska ske av användare som har behörighet till flera verksamheter.

Exempel på anledning till andra riktade loggkontroller av medarbetare kan vara släktrelationer eller annan nära relation till patienten/boende men där ingen aktuell vårdrelation till patient/boende föreligger. Där spärrar forcerats eller åtkomst skett över behörighetsgränser samt vid ett stort antal gånger avseende en viss patient.

Granskningsprotokoll för systematisk stickprovskontroll

Ett protokoll som dokumenterar att granskning har skett ska föras på en särskild blankett och arkiveras inom verksamheten. ”Granskningsprotokoll för systematisk stickprovskontroll”.

Blankett 4.5.1 Loggkontroll

- All loggranskning ska dokumenteras.
- Protokollet ska kunna visas upp vid uppföljningen av loggkontroller som sker i samband med kvalitetstillsyn av MAS.
- Granskningsprotokollet sparas i 10 år.

Granskningsresultat - vid ingen obehörig åtkomst till dokumentationssystemet

Visar uppföljningen av loggkontrollen ingen misstanke om obehörig åtkomst till vårdinformation noteras detta i rapporten för kvalitetstillsynen.

Granskningsresultat - behov av vidare utredning

Bedöms något som oklart tar verksamhetschefen kontakt med den användare det gäller.

Bedöms det efter utredning att det inte finns någon misstanke om obehörig åtkomst till vårdinformation kan ärendet dokumenteras och avslutas.

Om inte en godtagbar förklaring kan lämnas ska ärendet hanteras som ett arbetsrättsligt.

Visar analysen att det varit ett faktiskt dataintrång eller olovlig läsning ska ställningstagande till arbetsrättsliga åtgärder övervägas. Stöd för detta regleras i Allmänna bestämmelser (AB01) och kan t.ex. innebära avstängning med eventuellt avsked, varning med disciplinpåföljd eller enskilda samtal. Som disciplinpåföljd kan vara behörighetsbegränsningar och riktade loggkontroller under viss tid.

Om överträdelsen bedöms så allvarlig att den kan strida mot svensk lagstiftning, ska ärendet polisanmälas av verksamhetschefen.

Vid ett faktiskt dataintrång eller olovlig läsning ska detta dokumenteras i en avvikelserapport och verksamhetschefen ska kontrollera att verksamhetens rutiner – instruktioner, information samt förekommande utbildning är tydliga och kända hos alla medarbetare.

* **Blankett 4.5.1** Loggkontroll – granskningsprotokoll för systematisk stickprovskontroll

Regelverk

SFS 2010:659 Patientsäkerhetslag

SFS 2008:355 Patientdatalag

SFS 1998:204 Personuppgiftslag

SFS 1982:763 Hälso- och sjukvårdslagen

SOSFS 2011:9 Föreskrifter och allmänna råd för Ledningssystem för systematiskt kvalitetsarbete

SOSFS 2008:14 Föreskrifter och allmänna råd för Informationshantering och journalföring i hälso- och sjukvården

SOSFS 1997:8 Socialstyrelsens allmänna råd om verksamhetschef inom hälso- och sjukvård