



Riktlinje för loggkontroll i Pulsen Combine

Dokumenttyp Riktlinje	Dokumentnamn Riktlinje för loggkontroll i Pulsen Combine	Fastställd/uppriktad Kommunstyrelsen 2022-08-05	Beslutsinstans Kommunstyrelsen	Giltighetstid Tillsvidare
Dokumentansvarig Utvecklingsledare	Version 1.1	Senast reviderad Kommunstyrelsen 2024-04-08 § 43.	Dokumentinformation Dnr Ks 2022/497, 779.	Detta dokument gäller för handläggare, enhetschefer och utförare inom omsorg för äldre och funktionshindrade

Innehåll

1. Inledning	3
1.1 Syfte	3
2. Lagstiftning och föreskrifter	3
3. Ansvar	4
4. Kontrollrutiner	5
5. Flödesschema tolkning av logg.....	7
6. Granskningsresultat.....	8
6.1 Granskningsprotokoll för systematisk stickprovskontroll.....	8
6.2 Ingen misstanke om obehörig åtkomst till verksamhetssystemet	8
6.3 Granskningsresultat – behov av vidare utredning	8
7. Tidsschema för systematisk stickprovskontroll	9
8. Uppföljning av denna riktlinje	9

1. Inledning

Riktlinjen vänder sig till vård- och omsorgsverksamhetens område för äldre och funktionsvarierade. Riktlinjen beskriver hur ansvarsfördelningen ser ut i utförandet av loggkontroller och hur behörighetsstyrningen skall ske i Pulsen Combine. Vårdgivaren har enligt patientdatalagen ett uttalat ansvar för behörighetsstyrning och att föra logghistorik.

1.1 Syfte

Syftet med loggkontroll är att granska att vårdtagare/brukares integritet säkerställs samt att regelverket följs och att ingen otillbörlig användning av systemet sker. Kontrollen ska ske på ett systematiskt och regelbundet sätt.

Medarbetare som tilldelas behörighet till systemet ges en teknisk möjlighet att ta del av information angående vårdtagare/brukare. Detta innebär att möjligheten föreligger att ta del av information som man inte är behörig att ta del av.

Behörigheten till systemet styrs via två faktorsinloggning med e-postadress och lösenord samt FortiToken. 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 hur 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.

2. Lagstiftning och föreskrifter

Behov av logguppföljning (loggning) följer av säkerhetskraven i dataskyddsförordningen. Enligt offentlighets- och sekretesslagen (OSL) gäller även sekretess mellan olika verksamhetsgrenar inom en myndighet när de är att betrakta som självständiga i förhållande till varandra.

Ytterligare bestämmelser följer patientdatalagen och socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården (HSLFS 2016:40) där det framgår att den som arbetar hos en vårdgivare får ta del av dokumenterade uppgifter om en vård och omsorgstagare endast om han eller hon deltar i vården av den enskilde eller av annat skäl behöver uppgifterna för sitt arbete inom hälso- och sjukvården. Här regleras också vårdgivarens ansvar för kontroll av åtkomst till uppgifter.

För socialtjänstens verksamhet framgår behovet i socialtjänstlagen samt lagen och förordningen om behandling av personuppgifter inom socialtjänsten. Behov av loggkontroll nämns även i Socialstyrelsens handbok för ”Handläggning och dokumentation inom socialtjänsten” där nämnden benämns ansvarig att utarbeta rutiner för detta ändamål.

3. Ansvar

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

Enhetschefen är ansvarig för att informera personalen om att loggkontroll sker vilket ska ha en preventiv effekt. Personalen behöver informeras om det egna ansvaret, det vill säga under vilka omständigheter de får och ska ta del av brukar-/patientuppgifter och om följderna av att olovligen ta del av vård- och omsorgstagares uppgifter.

Enhetschefen ansvarar för att:

- Meddela objektspecialist vilken personal som ska ha vilken roll och inom vilken organisation.
- Meddela IT-enheten när personen slutat. Användaren avslutas automatiskt i Pulsen Combine när IT-enheten avslutar personen i Active Directory (AD).
- Via loggkontroll följa upp och kontrollera att användare följer de regler och rutiner som gäller för åtkomst till uppgifter angående vårdtagaren/brukaren.
- Varje användare informeras om loggning och loggkontroll utförs samt konsekvenser vid överträdelse
- Personalen är informerad om gällande lagstiftning och bestämmelser som gäller för hantering av uppgifter/information om vårdtagare/brukare i verksamhetssystemet.
- Följa upp så att informationshantering och journalföring i verksamhetssystemet har god kvalitet och är ändamålsenlig enligt gällande lagstiftning
- Initiera loggkontroll vid misstanke om obehörig åtkomst till dokumentation samt andra riktade loggkontroller

Medicinskt ansvarig sjuksköterska ansvarar för att:

- Det finns riktlinjer för loggkontroll i hälso- och sjukvårdsdokumentationen.

Objektspecialist ansvarar för att:

- Fördela roller och behörigheter i verksamhetssystemet för legitimerad personal och omsorgspersonal
- Tillsammans med enhetschef granska att tillgång till uppgifter angående vårdtagare/brukare används enligt gällande regelverk.
- Att ta ut loggar till enhetschefer som de ska granska.

Användaren ansvarar för att:

- Ta del av- och vara uppdaterad om rutiner och regler och följa dessa.
- Rapportera till närmaste chef om brister i rutiner eller om oegentligheter upptäcks.
- Kontrollera att rätt behörighet har tilldelats.
- Personliga lösenord och FortiToken inte kan bli tillgängliga till obehöriga.
- Datorer och annat informationsmaterial, såsom telefoner eller USB-minnen som har använts inte lämnas utan att uppgifterna angående vårdtagare/brukare är skyddade från obehörig åtkomst.
- Endast ta del av uppgifter angående vårdtagare/brukare som man deltar i vården av vårdtagare/brukare eller av något annat ändamål som anges i gällande regelverk då man behöver uppgifterna för sitt arbete.

4. Kontrollrutiner

1. Systematisk stickprovskontroll

Kontrollen skall ske inom Socialförvaltningen eller den modell som beskrivs under Tidsschema för systematisk stickprovskontroll. Loggarna skall granskas under en 24-timmarsperiod. Antalet användare som kontrolleras bör omfatta så många att det motsvarar sannolikheten att varje användare blir granskad minst en gång per år. Vid varje granskningstillfälle ska ett antal journaler (10 %) slumpmässigt väljas ut och granskas.

2. Vid vårdtagarens/brukarens begäran om loggutdrag

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

Den information om loggarna som lämnas ut ska vara anpassad till och klargörande för vårdtagare/brukare och det ska framgå vilken verksamhet och vid vilken tidpunkt någon har tagit del av uppgifterna. Dokumenteras i journalen.

3. Kontroll vid misstanke om obehörig åtkomst till vårdinformation

Vid misstanke om obehörig åtkomst till information ska loggkontroll omedelbart ske. 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 vårdtagare/brukare om det rör sig om en offentlig person eller att det finns en vårdtagare/brukare som är involverad i en händelse som kan bli massmedialt uppmärksammas.

4. Andra riktade loggkontroller – personal

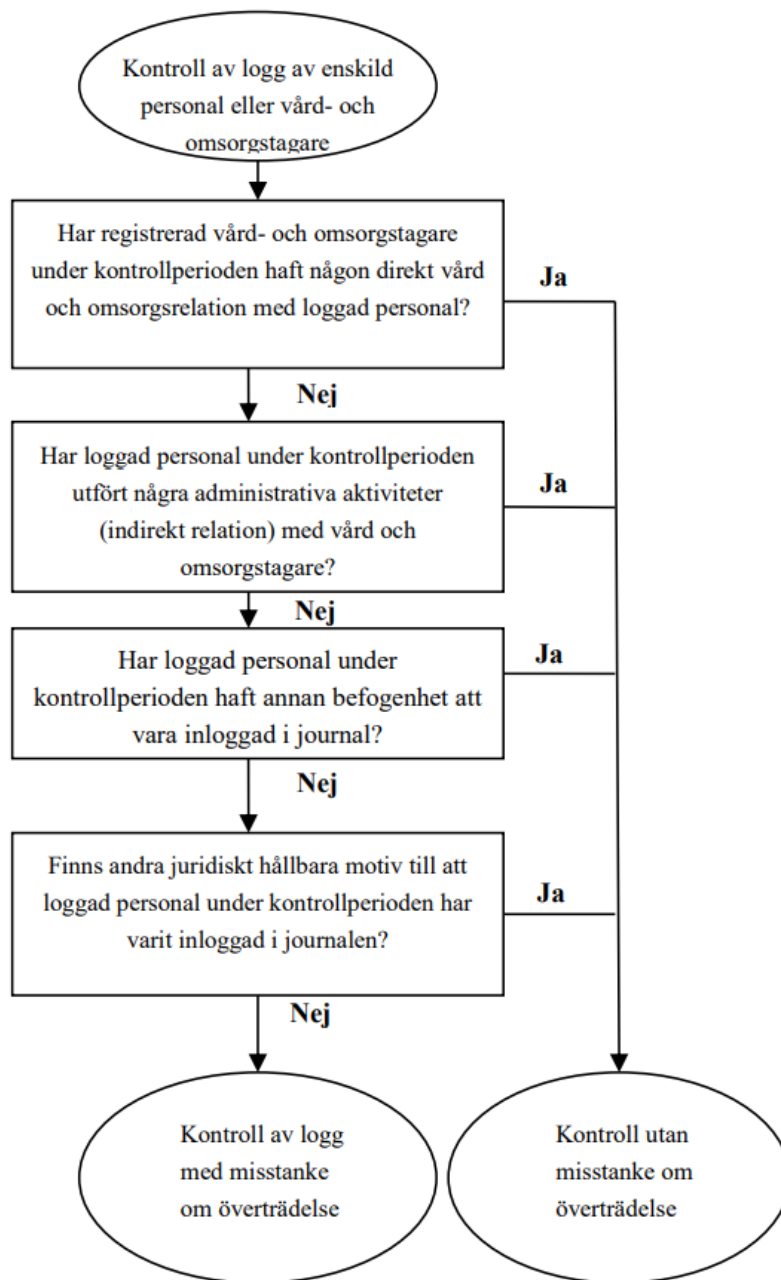
Särskild kontroll ska ske av användare som har behörighet till flera verksamheter. Exempel på anledning till andra riktade loggkontroller av medarbetare kan vara släktrationer eller annan nära relation till vårdtagare/brukare men där ingen aktuell vårdrelation till vårdtagare/brukare föreligger.

5. Andra riktade loggkontroller – dokumentation

Särskild kontroll ska ske av genomförandeplaner och journaler hos alla verksamheter. Exempel på anledning till andra riktigare loggkontroller av dokument kan vara att säkerställa att det finns:

- Aktuella vårdplaner och genomförandeplaner.
- Myndighet- och verkställighetsjournalanteckningar och andra handlingar som upprättas och som hör till den enskildes personakt ska vara väl strukturerade och tydligt utformade. Begrepp som används i dokumentationen ska vara så långt som möjligt vara entydliga. Av de upprättade handlingarna ska det framgå vad som är faktiska omständigheter och händelser av betydelse ska även innehålla uppgifter om när händelsen har inträffat. Av varje upprättad handling ska det framgå varifrån uppgifterna kommer, vem som har upprättat den och när det gjordes.
- Åtgärder som vidtas vid handläggning av ett ärende eller vid genomförande eller uppföljning av en insats ska fortlöpande och utan oskäligt dröjsmål dokumenteras i journalen.

5. Flödesschema tolkning av logg



6. Granskningsresultat

6.1 Granskningsprotokoll för systematisk stickprovskontroll

Ett protokoll som dokumenterar att granskning har skett ska föras på en särskild blankett och arkiveras inom verksamheten.

- All loggranskning ska dokumenteras.
- Protokollet ska kunna uppvisas vid uppföljningen av loggkontroller som sker i samband med intern kontroll.
- Granskningsprotokollet sparas på enheten i 10 år.

6.2 Ingen misstanke om obehörig åtkomst till verksamhetssystemet

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

6.3 Granskningsresultat – behov av vidare utredning

Bedöms något som oklart tar aktuell chef kontakt med den användare det gäller. Bedöms det efter utredning inte finnas 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 ärende.

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 berörd chef.

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

7. Tidsschema för systematisk stickprovskontroll

ROLLER I SYSTEMET	DATAURVAL	KONTROLLERAS AV	MINSTA FREKV/MÅN	MÄNGD	ANTAL %
Administratörer/ Systemansvarig	Allt	Socialchef	1 ggr/6 mån	1 dag	Alla
MAS	Allt	Socialchef	1 ggr/6 mån	1 dag	Alla
Avgiftshandläggare	Allt	Socialchef	1 ggr/6 mån	1 dag	Alla
Handläggare SOL/LSS	Allt	Socialchef	1 ggr/6 mån	1 dag	Alla
Socialsekreterare IFO	Allt	Socialchef	1 ggr/6 mån	1 dag	Alla
Sjuksköterska/ Arbetsterapeut/ Fysioterapeut	Allt	Enhetschef	1 ggr/ 6 mån	1 dag	50 %
Omsorgspersonal	Allt på enheten	Enhetschef	1 ggr/6 mån	1 dag	25 %

8. Uppföljning av denna riktlinje

Uppföljning av denna riktlinje kommer att ske årligen.

Granskningsprotokoll journallogg

ENHET _____

Namn	Datum	Kommentar/anmärkning	Granskning utförd av