Region Halland

Gäller för: Region Halland

Loggkontroll av åtkomst till vårdinformation

Hitta i dokumentet

Syfte
Bakgrund
Krav på logg av åtkomst till vårdinformation
Ansvar för kontroll av logg
Genomförande
Processbeskrivning
Misstanke om dataintrång
Dokumentation, hantering och förvaring
Uppdaterat från föregående version

Syfte

Denna rutin styr hur loggning och loggkontroller av åtkomst till vårdinformation ska genomföras.

Bakgrund

För att leva upp till de krav som Patientdatalagen och föreskriften HSFL-FS 2016:40 ställer, ska regelbunden och systematisk loggkontroll av åtkomst till vårdinformation genomföras.

Att vårdpersonal har tillgång till den patientdata som behövs vid varje tillfälle är en förutsättning för en effektiv och säker vård. Detta ställer i sin tur krav på att all åtkomst till patientens vårdinformation loggas och att man i efterhand kan svara på vem som har registrerat uppgifter eller haft åtkomst till patientens information. Det handlar om att upprätthålla patientens rätt till integritet och ett starkt förtroende till att vårdpersonal följer de regler som finns för åtkomst till information.

Krav på logg av åtkomst till vårdinformation

När information skapas, ändras eller läses i IT-system ska detta vara spårbart i en logg som ska visar VEM som gjort VAD och NÄR enligt följande:

1. vilka åtgärder som har vidtagits med uppgifter om en patient
   - specifika aktiviteter som är reglerad i lag, t.ex forcering av spärr
2. vid vilken vårdenhet eller vårdprocess som åtgärderna vidtagits,
3. vid vilken tidpunkt som åtgärderna vidtagits,
4. användarens och patientens identitet framgår av loggarna,
5. loggarna sparas enligt gällande gallringsbeslut (10 år) och därefter gallras
6. loggarna bör överföras till central granskningstjänst (Monitor) (se nedan undantag).

Krav på kontroll av loggar

Det ska göras systematiska och återkommande stickprovskontroller av den åtkomst som förekommit. Det ska också göras kontroll vid misstanke om obehörig åtkomst. Dessutom har patienten rätt att begära utdrag på sin logg för kontroll.

För en centralisering av loggar och ett gemensamt ärendeflöde för kontroll av åtkomstloggar har regionen ett loggranskningsverktyg (Monitor). Genom att loggar från olika vårdinformationssystem granskas på ett samlat sätt ges bättre förutsättningar för att upptäcka avvikelser (kvalitet, effektiv)

Systematisk stickprovskontroll
Huvudregeln är att loggar från vårdinformationssystem ska överföras till loggranskningstjänsten och ingå i den systematiska stickprovskontrollen. Till dess att loggar finns tillgängliga i granskningstjänsten får dessa kontrolleras manuellt eller med stöd av verktyg i det aktuella systemet.

Undantag från systematisk stickprovskontroll
Det finns även vårdinformationssystem som innehåller mycket begränsad mängd patientdata eller tjänster som har starkt begränsad behörighetstilldelning (t.ex vissa MT-system). För dessa tjänster bedöms det som tillräckligt att kontroll sker vid misstanke samt att patienten kan begära utdrag.

Ställningstagande till undantag av systematisk stickprovskontroll görs mellan informationsägare och applikationsägare för Monitor i samråd med informationsägare och applikationsägare för respektive system/tjänst.

Ansvar för kontroll av logg

Grundprincipen är att den som har rätt att dela ut behörigheter har också skyldighet att se till att loggkontroller genomförs och granskas.

Verksamhetschef
Verksamhetschef (eller motsvarande) har det övergripande ansvaret för att kontroll av loggar utförs enligt denna rutin inom sin verksamhet.

Varje medarbetare ska vara informerad och medveten om att all åtkomst till vårdinformationssystem loggas och granskas så att rutinen verkar proaktivt. Medarbetare ska också vara väl medvetna när det är tillåtet och inte att ta del av vårdinformation. Se rutin.

Ansvaret innebär även att fastställa omfattning för sin verksamhet genom att bedöma om omfattningen kan anses tillräcklig i förhållande till de lagkrav som finns och vad som hittas (risk/incidentfrekvens).

Enligt ovanstående grundprincip är loggranskningstjänsten utformad så att ärendeflödet följer strukturen i Hallandskatalogen (HAK). Utfall av granskning går för bedömning till chef för den verksamhet som granskas vid urval av patient. Vid anmärkning av medarbetare som tillhör annan verksamhet ska ärendet delges till berörd chef. Vid anmärkning av användare som tillhör eller har uppdrag på annan verksamhet ska ärendet delges till berörd chef. Gäller också inhyrd personal, timanställd och studenter

Loggranskare
Verksamhetschef alternativt underliggande chef ska tilldela uppdrag som loggranskare för verksamheten till minst två personer, se blankett: *Loggranskare - Uppdrag*

- Loggranskaren ska genomföra slumpvisa kontroller av patienter och medarbetare samt analysera resultat.
- Genomföra riktade kontroller på begäran av avd/verksamhetschef.
- Ta fram loggutdrag på begäran av patient enligt rutin: *Loggutdrag till patient*

Loggranskaren en har möjlighet att rekommendera ökad eller minskad omfattning av loggkontroller utifrån de faktiska utfallen. De har också till uppgift att hitta effektiva metoder och utvärdera utifrån önskad täckning, effektivitet och rationella arbetsformer.

Genomförande

Urval för kontroll görs med hjälp av slumpvalsgenerator i granskningsverktyget.

1. Loggranskaren skapar ärende i Monitor och granskar loggposterna och gör en analys av utfall. Följ manual Monitor - Loggningsverktyg

2. Ärendet notifieras till chef som godkänner eller initierar vidare utredning enligt rutin Dataintrång-Brott mot tystnadsplikt-Sabotage mot it-system-misstanke om

3. Vid anmärkning av loggpost som hör till annan chef notifieras denna för vidare kontroll.

Slumpvis kontroll
Varje vecka slumpas det fram medarbetare eller patient och logg från en 24-timmarsperiod tas fram för granskning.

Omfattningen av granskningen ska bedömas av verksamhetschef enligt ovan. Som ett minimum ska granskning genomföras;

verksamheter med journalansvar
Minst 1 patient per 50 anställda per vårdenhet ska granskas varje vecka.

verksamheter utan journalansvar
(exempelvis IVA, Akutklinik samt ej direkt vårdverksamhet som IT- och digitalisering, MTH med flera). Minst 1 medarbetare per 50 anställda per vårdenhet, mottagning eller avdelning granskas varje vecka.

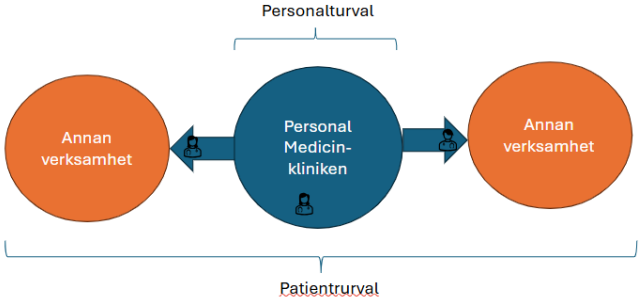
Särskild kontroll
Utöver slumpvis kontroll ska så kallad särskild loggkontroll göras vid misstanke om obehörig åtkomst. Behov av att genomföra särskild loggkontroll kan initieras av exempelvis patient, närstående, media, personal men beslut om att genomföra kontroll tas av chef.

Andra situationer då det kan vara lämpligt att göra en särskild kontroll är exempelvis:

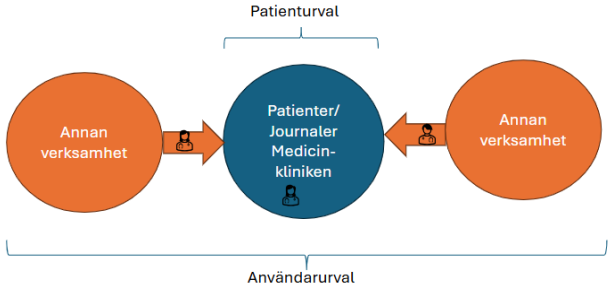
- Patienten har skyddade personuppgifter
- Patienten är lokalt och eller medialt känd
- En uppmärksammad olycka eller händelse
- Det finns en uttalad hotbild mot patient

- Patienten har en specifikt integritetskänslig diagnos

Urval vid granskning
Vid kontroll av personal inom den egna verksamheten fångar loggutdraget åtkomst både vid den egna verksamheten och i andra verksamheters journal.



Vid kontroll av patient inom den egna verksamheten fångar loggutdraget åtkomst både från den egna verksamhetens användare och åtkomst från andra verksamheters användare.



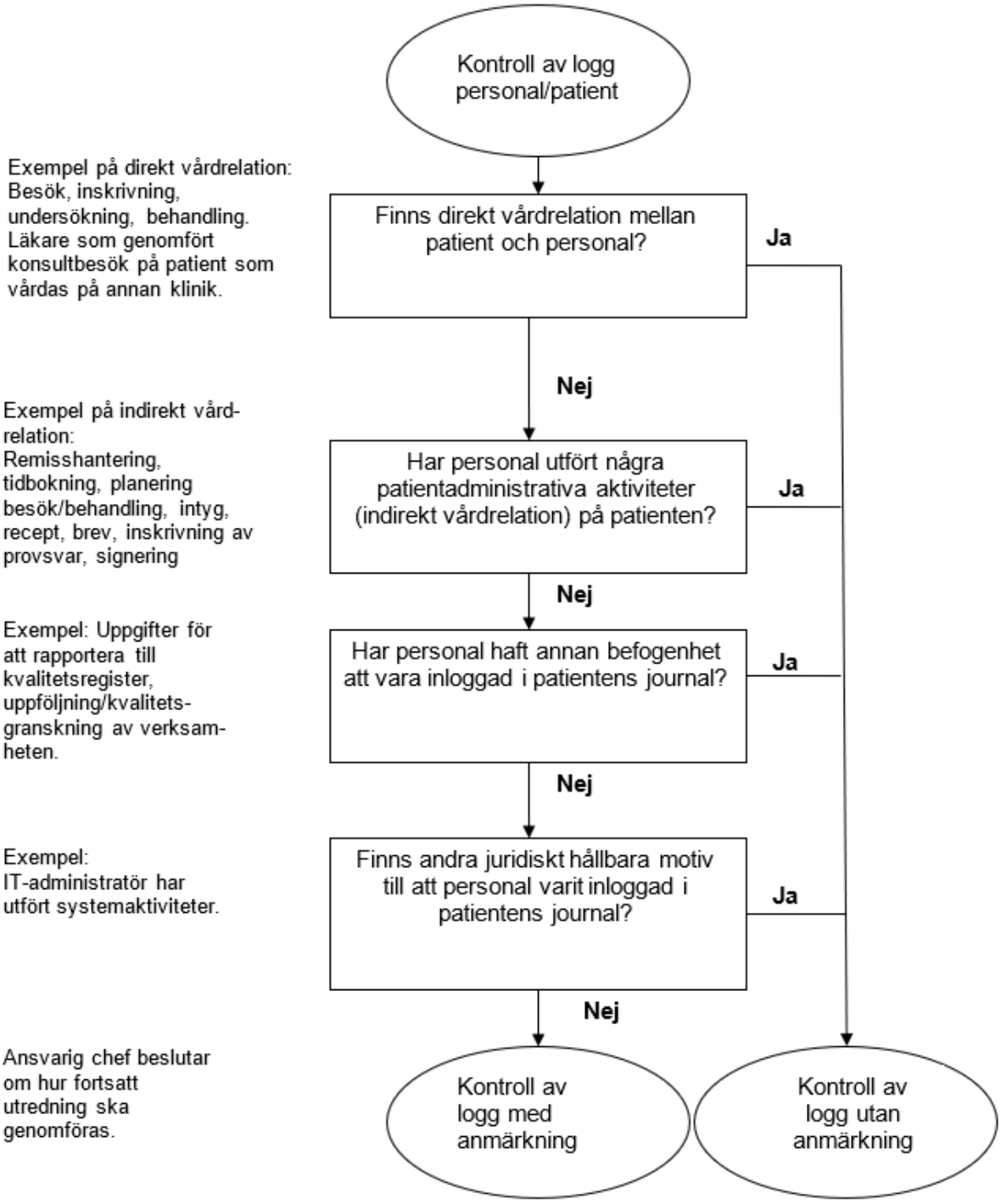
Vid anmärkning av loggpost som hör till annan verksamhet/chef överförs det för vidare kontroll av den som är chef för medarbetaren för vidare kontroll.

Analys
Kontrollera loggutdragen utifrån om det finns åtkomst som tyder på att det inte har funnits en relevant vårdrelation exempelvis följande punkter:

- Tidpunkter (t ex avvikande klockslag, utanför enhetens öppethållande, utanför personalens schema)
- Patientrelation/uppdrag (t ex patienter som inte är inskrivna på enheten, eller inte har besök bokat/registrerat.)
- Utförd aktivitet (där det framgår från loggutdrag - läsning är av större intresse, vid övriga aktiviteter såsom skriva, signera är patientrelation mer självklar)
- Avvikande mönster (åtkomst som bryter det ordinarie mönstret/frekvensen/rutinen)
- Namn/släktskap (åtkomst som indikerar privat samhörighet istället för patientrelation)
- Patienter av medialt intresse
- Patient med diagnos som kan väcka särskilt intresse

- Patient som är lokalt känd såsom personal
- Nödöppningar (där det framgår från loggutdrag)
- Samtycke till sammanhållen journal i kombination med avvikande användande

Processbeskrivning



Misstanke om dataintrång

Om analys visar på misstanke om dataintrång följ rutin Dataintrång – brott mot tystnadsplikt, sabotage mot it-system - misstanke om

Dokumentation, hantering och förvaring

Loggar i patientjournalsystem ska sparas i minst tio år. Skälet är att straffansvar enligt Brottsbalken och Preskriptionslagen inte kan utkrävas längre tid än 10 år efter ett intrång.

Dokumentationen av loggkontrollen ska sparas i två år enligt informationshanteringsplan. Gallring sker automatiskt i Monitor.

Uppdaterat från föregående version

Rutinen uppdaterad i sin helhet då nytt centralt loggverktyg införts (Monitor)