

Pia Lundbom
Pia.lundbom@skane.se

BESLUT

Datum: 2019-11-12
Dnr: 1800025

1 (5)

Instruktioner om loggkontroll för granskning av åtkomst till patientuppgifter

Syftet med dessa instruktioner är att beskriva hur loggkontroller avseende åtkomst till patientinformation ska utföras i Region Skåne.

Härmed beslutas att

- Instruktioner om loggkontroll för granskning av åtkomst till patientuppgifter, fastställs.
- Tidigare ”Instruktion, Loggkontroll – granskning av åtkomst till patientuppgifter”, daterad 2013-07-01, upphör att gälla.

Pia Lundbom

Koncernkontoret

Området för krisberedskap, säkerhet och miljöledning

Malin Nyman
Informationssäkerhetsspecialist
malin.nyman@skane.se

INSTRUKTION

Datum: 2019-11-12



2 (5)

Instruktioner om loggkontroll för granskning av åtkomst till patientuppgifter

Syftet med dessa instruktioner är att beskriva hur loggkontroller ska hanteras i Region Skåne.

Målet är att loggkontroller utförs på ett korrekt sätt i alla Region Skånes verksamheter, så att patienter kan känna sig trygga med hur organisationen hanterar personuppgifter och uppgifter om hälsa.

Inledning

Patientdatalagen ger hälso- och sjukvårdspersonal en ökad möjlighet för åtkomst till patientuppgifter såväl inom Region Skåne som mellan vårdgivare. Detta ställer också krav på ökad spårbarhet och kontroll av vem som tar del av patientuppgifter. Uppföljning av loggar är viktigt för att tillgodose patientens integritet och för att upprätthålla förtroendet för hälso- och sjukvårdens hantering av patientuppgifter. Loggkontroll har också betydelse som preventiv åtgärd för att avhålla personal från att ta del av patientuppgifter som de inte behöver för att utföra sina arbetsuppgifter.

Verksamhetschef¹ har ansvar för tilldelning av behörighet samt för kontroll av personalens åtkomst till patientuppgifter. Verksamhetschef kontrolleras i sin tur av utsedd person med kännedom om verksamheten.

Denna instruktion utgår från nationellt överenskommen vägledning för loggkontroll² som antagits i Region Skåne. Syftet med denna instruktion är att uppnå gemensamma rutiner för genomförande av loggkontroller inom Region Skåne. Instruktionen riktas till verksamhetschefer och personal inom hälso- och sjukvård.

Förutsättningar

Behörigheter

Behörigheter för åtkomst i IT-stöd ska tilldelas av verksamhetschef utifrån en bedömning av vilka patientuppgifter som den enskilde medarbetaren behöver tillgång till för att kunna utföra sina arbetsuppgifter, se vidare i ”Instruktioner om styrning av behörigheter för åtkomst till uppgifter om patienter”, beslutad 2019-03-08, dnr 1800025.

Information

Verksamhetschef ska informera sin personal om

- att det endast är tillåtet att ta del av de patientuppgifter som är nödvändiga för att utföra arbetsuppgiften
- att loggkontroll görs av personals åtkomst till patientuppgifter
- att ta del av patientuppgifter utöver vad arbetet kräver innebär att man gör sig skyldig till dataintrång³

Informationen är viktig i preventivt syfte.

¹ Verksamhetschefen är den som har det övergripande ansvaret för verksamheten.

² Kontroll av åtkomst till patientuppgifter – loggranskning, www.vardgivare.skane.se/informationssakerhet >Instruktioner>Hantering av patientuppgifter>Logg och loggranskning

³ Dataintrång enligt Brottsbalk (1962:700) 4 kap. 9 c §

Delegering

I de fall då verksamhetschef väljer att delegera handläggningen av loggkontroll ska delegeringen vara dokumenterad. Personal som handlägger loggkontroll ska också följas upp. Verksamhetschefen ansvarar för att detta genomförs.

IT-stöd

Åtkomst till patientuppgifter ska kontrolleras i de IT-stöd som används i verksamheten.

Genomförande**Stickprovskontroll**

Personal ska slumpmässigt väljas ut varje månad för kontroll. Ett riktmärke är 10 % av personalen. Kontrollen kan delas upp på flera tillfällen under månaden. Personal som slumpats fram ska granskas under minst 24 timmar.

Kontrollera loggutdragen utifrån 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 bokad/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 (åtkomst som indikerar nyfikenhet istället för patientrelation)
- Patient med diagnos som kan väcka särskilt intresse (åtkomst som indikerar nyfikenhet istället för patientrelation)
- Patient som är lokalt känd på vårdenhet eller inom vårdgivaren såsom personal/tidigare anställd personal (åtkomst som indikerar nyfikenhet istället för patientrelation)
- Egen journal

Riktad kontroll

Riktad kontroll ska göras både utifrån personals och patients identitet och ska göras vid de tillfällen då någon av följande företeelser inträffar

- Misstanke om obehörig åtkomst (t ex särskild händelse, lokalt känd patient, specifik diagnos eller på initiativ av patient)
- Vid vård av patient med skyddade personuppgifter
- Vid nödöppning av annan vårdgivares journal genom sammanhållen journalföring (ospärrade uppgifter)
- Vid forcering av spärr, oavsett då forcering skett med samtycke eller nödöppning

Granska loggutdragen för att kontrollera om någon obehörig har tagit del av patientuppgifter. Ta hjälp av punkterna under stickprovskontroll ovan.

Kontroll av nödöppning och forcering av spärr

All nödöppning och forcering av spärr ska kontrolleras. Forcering av spärr ska kontrolleras oavsett om den skett via samtycke eller nödöppning. Om orsaken till forcering inte är tillräckligt tydlig måste eventuellt kontroll av samtycket ske. Detta genom att kontakt tas med den användare som forcerat, med patient eller på annat sätt, t ex via journalanteckning.

Loggutdrag på patients begäran

På patients begäran ska loggutdrag lämnas vilket kan resultera i att patient misstänker obehörig åtkomst och initierar en riktad kontroll.

Begäran om loggutdrag som inkommer handläggs av Journal- och arkivservice på Regionarkivet.

Dokumentera och rapportera

Den som handlägger loggkontroll ska rapportera resultatet löpande till verksamhetschef eller utsedd person.

Verksamhetschef ska vid misstanke agera enligt instruktion vid misstanke om dataintrång⁴.

Samtliga kontroller som genomförs ska dokumenteras övergripande i avsett formulär på Region Skånes intranät, på sidan "Registrering och sammanställning av loggkontroller". Detta oavsett hur kontroll initierats och dess resultat.

Uppgifterna kommer att utgöra underlag för uppföljning av loggkontroller i Region Skåne och sparas i 3 år.

⁴ Dataintrång – åtgärder vid misstanke om olovlig åtkomst, www.skane.se/informationssakerhet >Ledningssystem>Anvisningar, instruktioner/rutiner > Hantering av patientuppgifter