Gemensam rutin för åtkomstkontroll

Grundläggande bestämmelser

Varje vårdgivare ska se till att åtkomst till patientuppgifter i journalsystemen kontrolleras. För att kunna utföra kontroller, ska all åtkomst till journalsystem dokumenteras genom automatisk loggning. Vårdgivaren ska göra systematiska och återkommande kontroller av åtkomsten, för att kunna bedöma huruvida behandlingen av patientuppgifterna är förenlig med författningar och övriga regelverk **(systematisk loggkontroll)**.

Vårdgivaren ska säkerställa att det av dokumentationen av åtkomsten (loggarna) framgår vilka åtgärder som har vidtagits med patientuppgifterna. Vidare ska det av loggarna framgå vid vilken vårdenhet och vid vilken tidpunkt som åtgärderna har vidtagits. Loggarna ska även innehålla uppgift om användarens respektive patientens identitet. Vårdgivaren ansvarar för att loggarna sparas i minst tio år och att genomförda kontroller av loggarna dokumenteras.

På begäran av en patient ska varje vårdgivare lämna information om den åtkomst till uppgifter om patienten som förekommit; såväl elektronisk åtkomst (åtkomst inom vårdgivaren) som direktåtkomst (åtkomst från annan vårdgivare). Av informationen som vårdgivaren ska lämna till en patient om åtkomsten till dennes patientuppgifter **(riktade loggkontroller)**, ska det framgå från vilken vårdenhet och vid vilken tidpunkt någon har tagit del av uppgifterna. Informationen ska vara utformad på ett sådant sätt att patienten kan göra en bedömning av om åtkomsten har varit befogad eller inte.

Bestämmelser om kontroll av åtkomst till patientuppgifter och vad som är tillåten och otillåten åtkomst till patientuppgifter finns bland annat i
Patientdatalagen (2008:355, PDL)
Socialstyrelsens föreskrifter och allmänna råd (HSLF-FS 2016:40) om journalföring och behandling av personuppgifter i hälso- och sjukvården
Offentlighets- och sekretesslagen (2009:400, OSL).

Denna riktlinje ska tillämpas vid kontroll av åtkomst till patientuppgifter samt vid misstanke om dataintrång.

Systematiska loggkontroller

Systematiska och återkommande stickprovskontroller ska göras av åtkomsten till patientuppgifter i journalsystemen, för att kunna bedöma huruvida behandlingen av patientuppgifterna är förenlig med författningar och övriga regelverk.

För journalsystemet TakeCare utförs dessa kontroller bl.a. med hjälp av SALA, som är ett webbaserat verktyg för att underlätta logguppföljningen för verksamheterna. Med hjälp av SALA hämtas en gång i månaden automatisk information om åtkomst till patientuppgifter som gjorts i TakeCare av ett antal slumpmässigt utvalda användare på respektive enhet. För varje enhet ska finns utsedda signerare och kontrasignerare vars uppgift är att kontrollera och vid behov följa upp loggarna. Det är önskvärt att åtminstone signeraren är nära användarna på enheten, för att enklare kunna bedöma rimligheten till åtkomsten. Det ska även finnas utsedda reserver i den händelse att signeraren och/eller kontrasigneraren slumpas fram.

Framtagen av: RVLP, Regional vård- och läkemedelsprocess
Godkänd av: Susanne Bergenbrant Glas
Giltighetstid (from-tom): 2025-02-01 – 2026-02-01
Version: 1.1

Riktade loggkontroller

Vem kan begära loggutdrag?
Loggutdrag kan begäras av patient eller verksamhetschef/motsvarande. En patient ska ha möjlighet att få information om den åtkomst till uppgifter om patienten som förekommit. På motsvarande sätt ska verksamhetschefen ha, vid t.ex. misstanke om otillåten åtkomst till patientjournal, möjlighet att få loggutdrag för att kunna fullgöra sitt ansvar att kontrollera användares åtkomst till patientuppgifter.

Om patienten är under 18 år har vårdnadshavare, som huvudregel, möjlighet att begära loggutdrag för sitt barns räkning. En bedömning måste dock göras i varje enskilt fall, utifrån barnets ålder och mognad samt utifrån offentlighets- och sekretesslagen.

För vilken tidsperiod kan loggutdrag begäras?
Den som begär loggutdrag har möjlighet att avgränsa sin begäran till en viss angiven tidsperiod. Om ingen särskild tidsperiod anges, lämnas information om den åtkomst som förekommit från den 1 juli 2008 och framåt, dvs. från det datum då patientdatalagen trädde i kraft.

Loggutdraget innehåller även information om huruvida personal, som är anställda hos andra vårdgivare, har berett sig åtkomst till uppgifter journalsystemet. Detta redovisas genom en förteckning över vilka andra vårdgivare som har haft direktåtkomst till uppgifter om patienten.