

Råd

kontroll av åtkomst till patientuppgifter - loggranskning

Innehåll

1	Inledning	4
2	Legala förutsättningar	4
3	Syfte.....	4
4	Ansvar	5
5	Omfattning	5
	5.1 Systematisk stickprovskontroll	5
	5.2 Kontroll vid särskild händelse eller misstanke.....	6
	5.3 Kontroll efter nödöppning	6
	5.4 Patientens rätt till kopia av loggen	6
6	Uppföljning ur patientens perspektiv	6
	6.1 Rutiner vid patientförfrågan om logginformation	6
	6.2 Patientens kostnad för loggutdrag	7
7	Nödvändiga funktioner	7
8	Dokumentationskrav	7
9	Om otillbörlig åtkomst misstänks eller bekräftas	7
10	Utmaningen - verksamhetens planering och genomförande.....	8
11	BIF loggtjänst och logganalystjänst.....	8

Utgåvehistorik för dokumentet

Utgåva	Datum	Kommentar
1.0	2010-04-01	Första utgåva
1.1	2010-10-06	Dokumentet inlagt i korrekt mall, smärre språkliga korrigeringar

Arbetsgruppen för säkerhet (AL-S). har på uppdrag av Centrum för e-hälsa (Cehis - arkitekturledningen) tagit fram en genomlysning av lagstiftningens krav och den praktiska tillämpningen hos vårdgivare. Dokumentets syfte är att tjäna som vägledning för vårdgivare.

1 Inledning

Den nya regleringen ger ökade möjligheter för åtkomst till patientdata inom en vårdgivares ansvarsområde och även mellan vårdgivare. Samtidigt ställs tydligare krav på att det finns spårbarhet och kontroll över vem som haft åtkomst till uppgifterna.

En av de stora utmaningarna för vårdgivare är att motsvara den nivå på skydd av patientens integritet som lagstiftningen ställer. Det gäller främst krav på spårbarhet, uppföljning och möjlighet att ge patient del av uppgifterna med sådan tydlighet, att denne kan avgöra om felaktig åtkomst har förekommit eller ej. Dessutom har patienten fått möjligheter att själv välja att spärra vald information, inom en vårdgivare och även mellan vårdgivare och till kvalitetsregister. Detta stärkta integritetsskydd förväntas uppväga lagstiftningens möjlighet att, under angivna former, dela information med andra vårdgivare.

2 Legala förutsättningar

Patientdatalagen (**SFS 2008:355**) gäller sedan 1 juli 2008 och ersätter den tidigare patientjournalagen och vårdregisterlagen. Ändringar har också införts i sekretesslagen. Vidare har Socialstyrelsen givit ut nya föreskrifter som rör informationshantering och journalföring (**SOSFS 2008:14**). I patientdatalagen regleras bland annat de möjligheter en patient har att styra åtkomst till patientuppgifter, både inom en vårdgivare och också där åtkomst möjliggjorts mellan vårdgivare.

Specifikt regleras det som gäller direktåtkomst via sammanhållen journalföring. För vårdgivare bestämmer lagen förutsättningarna för tillgång till vårdinformation och, till skillnad från tidigare skrivning, regleras nu möjligheter att via direktåtkomst dela vårddokumentation med andra vårdgivare.

Vårdgivare ska självmant, regelbundet och kvalitetssäkrat granska personalens åtkomst till patientens information med syfte att säkerställa att bara den personal som har rätt att ta del av uppgifter, har haft åtkomst till dessa. Grunden för åtkomst till patientinformation är att behov av uppgiften finns för vård eller annan arbetsuppgift.

Ansvar för uppföljning av åtkomst till patientinformation och behörighetstilldelning är direkt kopplat till rollen verksamhetschef.

3 Syfte

Loggningskontroll ska säkerställa vårdgivarens trovärdighet gentemot patienter. Granskning ska göras i den omfattning att den avhåller från otillbörlig åtkomst till patientinformation. Loggen ska hålla en sådan kvalitet att arbetsgivaren ska kunna vidta arbetsrättsliga åtgärder samt polisanmäla vid dataintrång. Loggen är samtidigt ett verktyg som kan fria anställd från misstanke om dataintrång.

4 Ansvar

Verksamhetschefen har det direkta ansvaret för såväl att tilldela som att kontrollera behörigheter. Principen är att den som har rätt att utdela behörigheter också har en skyldighet att kontrollera loggarna. I ansvaret ligger också att de anställda ska ha fått information om gällande regler för åtkomst till patientuppgifter och att rutinen för loggningskontroll är känd.

Verksamhetschefen kan delegera handläggningen till annan person inom vårdenheten. Vid delegering ska läggas vikt vid utförarens noggrannhet och denne ska ha en ställning i organisationen som innebär god personkännedom om enhetens personal.

Rutinen ska säkerställa att även utsedda granskare och verksamhetschefen själv granskas av överställd personal. Loggarna ska omfatta all åtkomst – dvs. även administrativ och teknisk personal ingår. Ansvaret för att loggningskontrollera åtkomst för personal som inte hör till någon verksamhetschef, faller på den som har ansvaret för att tilldela personen behörigheter. Personuppgiftsombud och patientnämnd kan på uppdrag från patient eller personal, ställa frågor om åtkomsten till patientinformation varit relevant och skett inom ramen för verksamhetschefens riktlinjer för åtkomst och behörighetstilldelning.

5 Omfattning

Kravet på loggningskontroll avser åtkomst inom vårdgivarens inre sekretessområde och direktåtkomst vid sammanhållen journalföring. Kravet omfattar alla typer av patientuppgifter. Loggningskontroll ska göras i den omfattningen att den är förebyggande och meningsfull. Detta uppnås genom en kombination av i huvudsak fyra skäl att göra loggningskontroll.

- systematisk stickprovskontroll
- Utöver den systematiska stickprovskontrollen ska loggranskning utföras: vid särskild händelse eller misstanke
- efter nödöppning
- på patientens begäran om utdrag av sin logg

5.1 Systematisk stickprovskontroll

Ett slumpmässigt urval av personalen ska med regelbundna tillfällen loggningskontrolleras, en rekommendation är att 10 % personal kontrolleras per månad, t.ex. uppdelat på 1-2 gång/månad. Den personal som slumpats fram granskas under en 24 timmarsperiod genom att all åtkomst till patientuppgifter visas upp. Följande kriterier är förslag på vad den som granskar loggen bör vara uppmärksam på:

- avvikande mönster/åtkomst som bryter det ordinarie mönstret/frekvensen/rutinen
- namn/släktskap som kan indikera privat samhörighet
- personer av medialt intresse, lokalt och nationellt
- patient med diagnos som kan väcka särskilt intresse
- lokal personalkännedom som indikerar eller ger misstanke om intresse för
- information som sträcker sig utanför tillåtna ändamål

5.2 Kontroll vid särskild händelse eller misstanke

Verksamhetschefen (arbetsgivaren) är skyldig att initiera loggningskontroll om det finns skäl att misstänka att dataintrång har skett. Det kan också finnas skäl att kontrollera loggen för en speciellt sekretesskänslig patient eller vårdepisod. Om man vid sådan kontroll uppmärksammar tveksam åtkomst av användare som hör till annan verksamhetschef så ska detta följas upp av den som tilldelat behörigheten.

5.3 Kontroll efter nödöppning

De aktiva val som föregår nödöppning eller forcering av spärr ska loggas. Det är lämpligt att sådan åtkomst granskas av verksamhetschef eller delegerad handläggare snarast. En obligatorisk logggranskning av nödöppningar är viktigt både ur ett integritetsperspektiv och för den kvalitetsgranskning som verksamhetschefen utför.

5.4 Patientens rätt till kopia av loggen

Patienten har rätt att få en kopia av sin logg. Dessa uppgifter ska vara så tydligt utformade att patienten kan bedöma om åtkomsten till patientuppgifterna varit befogade eller inte. Detta förutsätter att de aktörer som har haft tillgång till informationen är angivna på ett sådant sätt att bedömningen blir verkningsfull. Det innebär att hälso- och sjukvårdspersonals identitet och yrkesroll/tillhörighet syns i patientens logginformation i normalfallet. Om vårdnadshavare begär kopia av logg för barn bör, med hänsyn till stigande mognad och insikt hos barnet, en menprövning göras.

6 Uppföljning ur patientens perspektiv

Patienten ska känna stor förvissning om att vårdgivaren säkerställer att integritetsfrågan hanteras på ett ur både lagstiftningskrav och patientens önskemål korrekt sätt.

Vårdgivaren säkerställer att tillgången till information är behovsreglerad med individuell tillgångsprövning, och att den åtkomst som har skett är föremål för uppföljning.

Denna systematiska uppföljning sker automatiskt och metodiskt. Patienter har rätt att själv ta del av den åtkomst till information som har förekommit, för att trygga vetskapen om att ingen som inte har haft direkt behov av uppgifter har tagit del av dessa. Patienter har även rätt att spärra tillgång till information, både inom en vårdgivares enheter och i de fall vårdgivaren tillämpasammanhållen journalföring.

6.1 Rutiner vid patientförfrågan om logginformation

Det ska finnas information på lämpliga ställen om vart patienten vänder sig för att få en kopia av loggen. Patienter kan ställa frågor direkt till klinik/enhet, personuppgiftsombud, patientnämnd eller myndighetsbrevlåda. Det är lämpligt och praktiskt för både vården och patienten att det finns ett formulär som kan användas. Med hjälp av detta kan förfrågan preciseras så att patienten får det denne efterfrågar. Det kan också vara lämpligt att ta en direktkontakt med patienten för att säkerställa tillgång till annan relevant information och om så önskas hjälpa patienten med att avgränsa till de enheter som patienten avser.

Patienten bör få svar skyndsamt eftersom loggar utgör en allmän handling. I normalfallet sker utlämnandet i pappersform. Uppgifterna skickas till patienten på dennes folkbokföringsadress eller kan lämnas ut direkt om patienten har legitimerat sig. De logguppgifter som lämnas till patient bör även lämnas till verksamhetschef för kännedom.

Loggutdraget ska vara utformat så att det ger patienten en klar uppfattning om åtkomsten till dennes patientuppgifter. Patientens fråga om vem som har sett information är ibland baserad på en specifik händelse eller uppgift, där patienten upplever att någon har information som inte patienten bedömer ska vara tillgänglig. I sådant fall ska, på patientens begäran, analys ske av den berörda medarbetaren och dennes tillgång. Personuppgiftsombudet ska vara patientens stöd och skapa rutiner för att patientförfrågan hanteras rätt i vårdgivarens organisation.

6.2 Patientens kostnad för loggutdrag

Respektive vårdgivare beslutar om det ska tas ut avgift och nivån på denna. En rekommendation är att kostnaden hålls så låg att den inte innebär hinder för patienten att få utdrag. Patienten är en resurs för vårdgivaren i dennes granskning av loggar.

7 Nödvändiga funktioner

Tillgång till logg och logganalysverktyg ska regleras med individuell behörighetstilldelning och begränsas till dem som har ett särskilt uppdrag att granska loggar.

Utöver patientens och användarens identitet ska det i klartext framgå vilka åtgärder (läsa/skriva/ändra/signera/kopiera/utskrift) som vidtagits med patientuppgifterna, vilken vårdenhet som vidtagit åtgärderna och tidpunkten för detta.

Hos vårdgivaren ansvarig roll i systemförvaltningsstruktur, säkerställer att nödvändig funktionalitet för uppföljning finns exempelvis aktiva val och forcering av spärr, och förser verksamhetschefen med nödvändigt stöd för loggranskning i respektive vårdsystem.

Den aktuella informationstexten /informationsinnehållet ska inte visas i loggen.

8 Dokumentationskrav

Loggranskning ska resultera i dokumentation som omfattar urvalet, grunden för urvalet (anmodan, eget urval, förekommen aktivitet etc) och resultat med kommentar. Om ingen otillbörlig åtkomst upptäcks rapporterar granskare till verksamhetschef med bifogat underlag löpande. Resultatet sparas enligt gällande arkivbestämmelser medan loggarna ska bevaras i 10 år.

9 Om otillbörlig åtkomst misstänks eller bekräftas

Om otillbörlig åtkomst misstänks ha förekommit ska underlag för detta lämnas verksamhetschefen i anslutning till upptäckten. Utredningen ska säkerställa detaljnivå och informationsinnehållet för läst vårdinformation. Vårdgivare måste säkerställa att respektive vårdsystem har interna loggar på detaljnivå.

Denna, i samråd med av vårdgivaren beslutade instanser, avgör vidare handläggning. Vid misstanke om otillbörlig åtkomst, ska loggranskning alltid genomföras. Det är viktigt, både för

patienten och för vårdgivaren, att misstanke om missbruk följs upp och utreds. Det kan även vara aktuellt att göra en fördjupad logggranskning av en medarbetare. Medarbetaren ska kontaktas och få möjlighet att förklara skälen till aktuell loggförekomst. Inför ett sådant samtal ska medarbetaren informeras om möjligheten att ta med en facklig representant.

Vid samtalet bör följande frågor besvaras:

- Varför har medarbetaren sökt information om denna patient?
- Känner medarbetaren patienten eller har någon annan anknytning med patienten privat?
- Vilken information har använts och till vad?
- Av vilken anledning har medarbetaren valt att bryta mot bestämmelserna i Patientdatalagen?

Vid bekräftad misstanke om dataintrång ska verksamhetschefen även informera berörd patient.

10 Utmaningen - verksamhetens planering och genomförande

Vårdgivarens systematiska uppföljning måste inrymmas i uppdraget till verksamhetschef och därmed ingå i de prioriterade uppgifter som vårdgivaren ålägger verksamhetschef.

Att på förhand sätta upp volymkrav i förhållande till patientmängd och verksamhetens omfattning innebär inte att syftet med uppföljning med automatik säkerställs.

Verksamhetschef måste ta ställning till vad en planerad granskning innebär för just sin verksamhet. Vilken typ av patientuppgifter hanteras, vilka överväganden ingick i den individuella behörighetstilldelningen (bredare behörighet ger ökat krav på uppföljning), vilka urval ger bäst möjlighet till hög sannolikhet för upptäckt av intrång, finns nödvändig information och underlag för att stödja uppföljningen. Verksamhetschefen kan ange omfattning och resultat av granskningsaktiviteter för enheten i sin verksamhetsberättelse.

Ett av de viktigaste syftena med uppföljning är att den är känd av berörd personal. Varje medarbetare med tillgång till patientuppgifter ska se denna granskning som ett naturligt inslag i vårdgivarens verksamhet samt att den medför en förebyggande effekt.

Logginformation och kontroll har även en viktig uppgift i att undanröja misstanke om felaktig åtkomst. Logguppgifter kan förväntas lika ofta eller kanske oftare fria från misstanke än bekräfta sådan.

Tillgång till logguppgifter kan som informationsmängd även innebära att en detaljerad bild av patienten kan framkomma. Detta ska ingå i den riskbedömning som föregår tillgång till logginformation.

11 BIF loggtjänst och logganalystjänst

För att använda BIF tjänsterna behöver vårdgivaren göra anpassningar i sina vårdssystem.

Loggtjänsten kvalitetssäkrar logginformation från olika vårdssystem och gör den tillgänglig i standardiserat format och struktur för logganalysttjänsten. Det är via logganalysttjänsten som verksamhetschef får stöd i uppföljningen. Det är en brist att analystjänsten inte innehåller ett färdigt utbud av standardmallar från start och utvecklade exempel på hur analysverktyget kan konfigureras. Loggtjänsten bör ha möjlighet att hantera i förväg satta "markörer" som signalerar att viss aktivitet bör granskas. En sådan markör kan vara att patientinformation öppnats utan att patienten är inskriven/besöksnotering eller har annan planerad kontakt.

6 oktober 2010

Förutom BIF tjänsterna kan andra analysverktyg användas av vårdgivare för att säkerställa uppföljning.