



Patientdatalagen och den personliga integriteten

Patientdatalagen innehåller en samlad reglering av informationshanteringen inom hälso- och sjukvården. Den nya lagen, som trädde i kraft 1 juli 2008, ersätter vårdregisterlagen och patientjournalagen och ska tillämpas av alla vårdgivare, både i offentlig och privat regi. I detta faktablad ger Datainspektionen en kort, översiktlig introduktion till lagen.

Nya möjligheter och tydligare krav

Nyheter i patientdatalagen är bland annat att det blir möjligt att ha sammanhållen journalföring mellan vårdgivare och att vårdgivaren har ett uttalat ansvar för behörighetsstyrning samt för att föra behandlingshistorik (loggar) och att följa upp loggarna. Den nya lagen ger patienter möjlighet att spärra uppgifter i journaler. Det blir också möjligt för vårdgivarna att ge patienten tillgång till sina uppgifter elektroniskt via exempelvis Internet. Nytt i patientdatalagen är också att det finns särskilda regler för hälso- och sjukvårdens kvalitetsregister.

Inre sekretess

En utgångspunkt för den inre sekretessen, integritetsskyddet inom en verksamhet, är att en användare endast ska få ta del av patientuppgifter som behövs för att han eller hon ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården. Den inre sekretessen tydliggörs genom regler om behörighetsstyrning och kontroll av elektronisk åtkomst samt patienters rätt att få information om elektronisk åtkomst och att begära spärrar. Inre spärrar innebär att åtkomsten till patientuppgifter i journalsystemet har begränsats genom att patienten själv har begärt en spärr. Patienten kan bara spärra uppgifter för andra vårdenheter och andra vårdprocesser hos samma vårdgivare. Det innebär att vårdgivaren behöver definiera vilka vårdenheter och vårdprocesser som finns i den egna verksamheten.



Datainspektionen

Aktiva val och spärrar vid inre sekretess

Vid inloggning i journalsystemet ska användaren endast se de patientuppgifter som härrör från den egna enheten eller den vårdprocess som användaren ingår i. Det ska framgå om det finns spärrade och/eller ospärrade uppgifter om patienten hos en annan enhet eller vårdprocess. För att få ta del av ospärrade uppgifter hos en annan vårdenhet eller vårdprocess krävs att användaren gör ett aktivt val. Det innebär att användaren först ska bedöma om uppgifterna är nödvändiga för att han eller hon ska kunna fullgöra sina arbetsuppgifter. Därefter ska användaren göra ett aktivt val i journalsystemet för att bekräfta bedömningen. Det aktiva valet ska loggas för att dokumentera bedömningen. För att få ta del av spärrade uppgifter krävs i normalfallet ett samtycke från patienten. Om patienten inte kan samtycka och användaren bedömer att uppgifterna kan antas ha betydelse för vård som patienten oundgängligen behöver (det vill säga en nödsituation föreligger) får spärran brytas. Användaren ska bekräfta sin bedömning genom att göra ett aktivt val i systemet.

Sammanhållen journalföring

Varje vårdgivare ska föra sina egna patientjournaler. Genom reglerna i patientdatalagen får vårdgivare möjlighet att ta del av andra vårdgivares journaluppgifter på ett smidigare sätt än tidigare.

Reglerna om sammanhållen journalföring gör det möjligt för en vårdgivare att elektroniskt ge eller få åtkomst till patientuppgifter hos en annan vårdgivare. Patientdatalagen reglerar dels hur en vårdgivare får göra patientuppgifter från den egna verksamheten tillgängliga för andra vårdgivare, dels hur en vårdgivare får ta del av andra vårdgivares patientuppgifter. Lagen ger dock patienten möjlighet att motsätta sig att hans eller hennes patientuppgifter ska ingå i sammanhållen journalföring, det vill säga spärra uppgifterna. Om det finns spärrade uppgifter får det, trots det, framgå att spärrade uppgifter finns samt vilken vårdgivare som spärrat uppgifterna.

För att patienten ska kunna tillvarata sina rättigheter ska vårdgivaren informera patienten om sammanhållen journalföring innan patientuppgifterna görs tillgängliga för andra vårdgivare. Patienten ska informeras om vad sammanhållen journalföring är och bör lämpligen även få information om vilka vårdgivare och vilka uppgifter som ingår, ändamålet med den sammanhållna journalföringen samt möjligheterna som finns att spärra uppgifter och om hur spärrar får hävas.

Det är den vårdgivare som tar del av andra vårdgivares patientuppgifter i den sammanhållna journalföringen som ansvarar för att uppgifterna hanteras enligt reglerna i patientdatalagen.

Aktiva val och spärrar vid sammanhållen journalföring

I ett system för sammanhållen journalföring ska en användare kunna ta del av information om att det finns spärrade och/eller ospärrade uppgifter om patienten hos andra vårdgivare som ingår i systemet utan att ta del av några patientuppgifter. För att en användare ska få ta del av ospärrade uppgifter om en patient krävs att följande förutsättningar är uppfyllda.

- Användaren har en aktuell patientrelation med patienten,
- uppgifterna kan antas ha betydelse för att förebygga, utreda eller behandla sjukdomar och skador hos patienten inom hälso- och sjukvården samt

- patienten samtycker till att vårdgivaren behandlar uppgifter som en annan vårdgivare gjort tillgängliga i systemet.

Om dessa förutsättningar är uppfyllda får användaren ta del av uppgifterna genom att göra ett aktivt val i journalsystemet. Det aktiva valet bekräftar att användaren bedömt att förutsättningarna är uppfyllda.

Om det föreligger fara för patientens liv eller allvarlig risk för patientens liv och patienten inte, på grund av till exempel medvetlöshet, kan samtycka kan en användare ändå få åtkomst till ospärrade uppgifter. Det förutsätter dock att användaren efter ett aktivt val först tar del av en lista över vilka andra vårdgivare som har uppgifter om patienten. Det aktiva valet bekräftar att användaren bedömt att det föreligger en sådan nödsituation. Med ledning av listan kan användaren därefter bedöma om uppgifterna kan antas ha betydelse för vård som patienten oundgängligen behöver. Användaren får ta del av de uppgifter som kan antas ha sådan betydelse genom att göra ett aktivt val i journalsystemet som bekräftar användarens bedömning. Det krävs alltså två aktiva val för att ta del av uppgifter i en nödsituation.

Huvudregeln i sammanhållen journalföring är att andra vårdgivare inte får ta del av spärrade uppgifter. Den vårdgivare som har lagt in spärren ska dock om patienten själv begär det häva spärren. I en situation då patienten själv inte kan häva spärren och det föreligger fara för patientens liv eller annars allvarlig risk för patientens hälsa (det vill säga en allvarlig nödsituation) kan den vårdgivare som behöver ta del av uppgifterna om patienten få tillgång till en lista över vilka andra vårdgivare som har spärrade uppgifter om patienten. Genom ett aktivt val i journalsystemet bekräftar användaren att han eller hon har bedömt att det är fråga om en sådan allvarlig nödsituation, exempelvis att patienten är medvetlös eller i ett sådant tillstånd att det inte finns tid att vänta på att patienten själv ska häva spärren. Om användaren med ledning av listan bedömer att uppgifter hos andra vårdgivare kan antas ha betydelse för den vård som patienten oundgängligen behöver får vårdgivaren begära att spärren hävs hos den vårdgivare som har spärrat uppgifterna. Det är alltså bara den vårdgivare som lagt spärren som kan häva den. Vid begäran från en annan vårdgivare får den vårdgivaren som lagt spärren endast häva den för detta enskilda tillfälle och bara beträffande de uppgifter som bedöms ha betydelse för den vård patienten oundgängligen behöver, även om spärren omfattar fler uppgifter.



Behörighetsstyrning och åtkomstkontroll

Vårdgivaren ska se till att behörigheten för åtkomst till patientuppgifter begränsas till vad en användare behöver för att kunna utföra sina arbetsuppgifter inom hälso- och sjukvården. Behörigheter ska fortlöpande följas upp och korrigeras utifrån eventuella förändringar i användarens arbetsuppgifter. En vårdgivare ska också dokumentera elektronisk åtkomst till patientuppgifter och systematiskt och återkommande kontrollera åtkomsten till patientuppgifterna. En sådan kontroll främjar integritetsskyddet och gör det möjligt att förebygga, konstatera och beivra otillåten eller obefogad åtkomst till uppgifter.

Bestämmelserna om behörighetstilldelning och åtkomstkontroll finns i patientdatalagen. De gäller både vid inre sekretess och vid sammanhållen journalföring. Kraven på säkerhetsåtgärder förtydligas i Socialstyrelsens föreskrifter (SOSFS 2008:14) om informationshantering och journalföring i hälso- och sjukvården. Föreskrifterna innehåller regler om informationssäkerhetspolicy, öppna nät, styrning av behörigheter, åtkomst till patientuppgifter, kontroll av åtkomst, säkerhetskopiering, enskildas åtkomst, med mera.

Patientens tillgång till logg och egna uppgifter

Vårdgivare har enligt patientdatalagen möjlighet, men ingen skyldighet, att ge patienten tillgång till sina egna patientuppgifter elektroniskt, till exempel via Internet. Detta förutsätter dock att vårdgivaren först bedömer vilka uppgifter det är lämpligt att lämna ut på detta vis. Vårdgivaren måste också vidta lämpliga säkerhetsåtgärder såsom till exempel säker identifiering av patienten med e-legitimation och kryptering vid överföringen av uppgifterna.

Vårdgivaren ska på begäran från patienten informera om den åtkomst till patientens uppgifter som förekommit. Vårdgivaren är skyldig att lämna ut informationen på papper och får, men har ingen skyldighet att, ge patienten direktåtkomst till informationen. Det förutsätter att säkerhetskraven är uppfyllda på samma sätt som vid patientens direktåtkomst till egna journaluppgifter. Patienten har dock bara rätt att på detta sätt få reda på vilken vårdenhet (men inte vilken användare) som haft åtkomst till uppgifterna och vid vilken tid. Informationen ska vara utformad så att patienten kan bedöma om åtkomsten var befogad eller inte.

Nationella och regionala kvalitetsregister

Patientdatalagen innehåller särskilda regler för hälso- och sjukvårdens kvalitetsregister. Dessa register används för att systematiskt och fortlöpande kunna utveckla och säkra vårdens kvalitet. De nya reglerna syftar till att ge ett starkare integritetsskydd för patienterna. Endast myndigheter inom hälso- och sjukvården får ansvara för och föra ett kvalitetsregister. Patienten har enligt lagen rätt att få information om registreringen samt rätt att slippa bli registrerad i ett kvalitetsregister och även rätt att stryka sig i efterhand.

Tillsyn

Datainspektionen har tillsyn över att vårdgivarna hanterar personuppgifterna med ett gott integritetsskydd för patienterna. Det innebär till exempel att Datainspektionen kan kontrollera att vårdgivaren vidtar säkerhetsåtgärder för att skydda patientuppgifterna, till exempel att vårdgivaren har rutiner för behörighetsstyrning och åtkomstkontroll. Socialstyrelsen är tillsynsmyndighet för journalföringen och kontrollerar till exempel innehållet i och hanteringen av journalhandlingar.

Kontakta Datainspektionen

E-post: datainspektionen@datainspektionen.se Webb: www.datainspektionen.se
Tfn 08-657 61 00. Postadress: Datainspektionen, Box 8114, 104 20 Stockholm.



Datainspektionen