Integriteten på den nya apoteksmarknaden

Det här informationsbladet vänder sig till dig som är kund hos ett apotek. Längre ner finns det också råd till de företag som driver apotek.

Information till dig som är apotekskund

Den 1 juli 2009 upphörde Apoteket AB:s monopol på att sälja läkemedel. Numera kan olika företag öppna så kallade öppenvårdsapotek som fungerar ungefär på samma sätt som de gamla apoteken. De nya apoteken måste ha tillstånd från Läkemedelsverket för att få sälja och ge råd om läkemedel och de måste följa apoteksdatalagen som trädde i kraft den 1 juli 2009. Ett öppenvårdsapotek måste också ha ett säkert elektroniskt system för att hantera kund- och receptregister.

Det centrala receptregistret

När du besöker en läkare eller sjuksköterska och får ett recept på ett läkemedel så sänds receptet elektroniskt till det så kallade centrala receptregistret. Tidigare var det Apoteket AB som hade ansvar för det registret och läkemedelsförteckningen men nu sköts detta av eHälsomyndigheten, som är personuppgiftsansvarig. Apotekspersonal har tystnadsplikt när det gäller hanteringen av uppgifter i receptregistret och hos eHälsomyndigheten gäller bestämmelserna om sekretess i Offentlighets- och sekretesslagen (2009:400).

Vem på de nya apoteken får läsa recept?

När du vänder dig till ett öppenvårdsapotek för att hämta ut mediciner kan personalen se ditt recept i receptregistret. De får också ta del av dina läkemedelsförmåner för att kunna räkna ut kostnaden. Öppenvårdsapoteket ska sedan skicka tillbaka uppgifter till receptregistret för att exempelvis landstingen ska faktureras på rätt sätt. På öppenvårdsapoteken har den personal som har hand om läkemedel eller ger dig råd tystnadsplikt.

Datainspektionen

September 2014

Endast behöriga personer hos öppenvårdsapoteken och eHälsomyndigheten får ta del av dina uppgifter och de får bara göra detta när det behövs i arbetet. Dessutom måste dessa företag göra kontroller av registrens så kallade loggfiler för att se så att inga dataintrång eller onödiga inloggningar har gjorts.

Kundklubbar
Utöver recepthantering förekommer det att apotek har kundklubbar för att registrera andra inköp i butiken. Om du handlat något tidigare och ditt apotek vill skicka reklam om liknande varor ska du få information om det. Då kan du välja om du vill samtycka till att apoteket anpassar utskicken efter dina tidigare inköp.

Information till apoteksmarknadens aktörer

Här följer information till apoteksmarknaden när det gäller några av de väsentliga säkerhetsåtgärder som behöver vidtas enligt lagen om receptregister, lagen om läkemedelsförteckning, apoteksdatalagen och personuppgiftslagen.

Apoteksmarknaden och informationssäkerheten
I och med omregleringen av apoteksmarknaden upphörde Apoteket AB:s monopol och ersattes med ett system där den som har fått tillstånd av Läkemedelsverket (tillståndshavaren) får bedriva detaljhandel med läkemedel. Handeln bedrivs på så kallade öppenvårdsapotek. Ett krav på ett öppenvårdsapotek är att ha ett elektroniskt system som gör det möjligt att få direktåtkomst till uppgifter hos eHälsomyndigheten. Läkemedelsverket har tagit fram föreskrifter som reglerar apoteksmarknaden och recepthanteringen.

eHälsomyndigheten och öppenvårdsapoteken får hantera känsliga personuppgifter i enlighet med lagen om receptregister och lagen om läkemedelsförteckning samt apoteksdatalagen. De är var och en personuppgiftsansvariga för sin hantering av personuppgifter. Det rör sig om mycket känslig information som omfattar en stor del av befolkningen. Säkerheten måste därför vara sådan att obehörig användning av uppgifterna inte förekommer. Lagarna innehåller uttryckliga krav på behörighetsstyrning och åtkomstkontroll (logguppföljning) men det finns också behov av andra säkerhetsåtgärder.

Datainspektionens allmänna råd om säkerhet för personuppgifter ger vägledning om andra säkerhetsåtgärder som måste vidtas. Apoteken behöver göra risk- och sårbarhetsanalyser till exempel innan nya hälsorelaterade tjänster införs. Datakommunikationen måste skyddas under överföringen av personuppgifter mellan eHälsomyndigheten och öppenvårdsapoteken. En oskyddad överföring av receptuppgifter innebär en avsevärd integritetsrisk. Fler åtgärder finns i de allmänna råden som du hittar på www.datainspektionen.se.

Information till apoteksanställda

En viktig del av integritetsskyddet är att användarna av IT-systemen informeras om vikten av att följa gällande säkerhetsrutiner och att de får konkreta instruktioner om hur personuppgifterna får hanteras. I det ingår att informera de anställda om att loggkontroller utförs och om de anställdas tystnadsplikt.

Informerar man de anställda om dessa förutsättningar har det en preventiv verkan och kan avhålla dem från att ta del av uppgifter när det inte behövs för att fullgöra arbetsuppgifterna. Att läsa kundernas recept och uppgifter om läkemedelsanvändning utan att behöva det för att utföra sina arbetsuppgifter är inte tillåtet. Den som gör detta kan göra sig skyldig till dataintrång.

Behörighetsstyrning

Lagarna anger att eHälsomyndigheten och tillståndshavarna ska bestämma och formulera villkoren för tilldelningen av behörigheter för åtkomst till uppgifterna i registren. Behörigheten ska begränsas till vad som behövs för att en användare ska kunna fullgöra sina arbetsuppgifter. Utgångspunkten är att alla användare inte behöver åtkomst till alla personuppgifter.

Varje användare ska få en individuell behörighet vilket innebär att så kallad gruppinloggning inte får användas. Tilldelningen av behörigheten ska bygga på att det har gjorts en behovs- och riskanalys av vilka uppgifter olika personalkategorier behöver ta del av och vilka risker det finns med det. Kretsen av personer som har tillgång till skyddade personuppgifter bör begränsas så mycket som möjligt. Det ska finnas rutiner för behörighetsstyrningen för att kunna göra löpande ändringar och ta bort inaktuella behörigheter.

Åtkomstkontroll

eHälsomyndigheten och tillståndshavarna ska se till att åtkomst till personuppgifter dokumenteras och att det sker systematiska och återkommande kontroller av om någon kommer åt personuppgifter på ett obehörigt sätt.

Det innebär att det ska finnas loggar som visar användaridentitet, tidpunkt och vilka personuppgifter användaren har haft åtkomst till och i vilken form, exempelvis läsning, ändring, utskrift eller kopiering. Loggarna ska följas upp för att upptäcka och utreda eventuell felaktig eller obehörig användning av personuppgifter. Det räcker inte att göra kontroller endast när det finns misstanke om obehörigt intrång.

Rutinen för kontrollerna ska vara utformad så att uppföljningen blir verkningsfull. Ett sätt kan vara att utforma kontroller som riktar in sig på vissa typer av uppgifter (till exempel sekretessmarkerade personuppgifter) eller åtkomst som sker utanför arbetstid.

Datainspektionens Checklista för hälso- och sjukvården – Systematisk loggupp-följning kan användas som ett stöd för kvalitetsutveckling av logguppföljningarna. Checklistan hittar du på www.datainspektionen.se/logguppfoljning

Säkerhet vid överföring
Ska man överföra personuppgifter som handlar om recept eller läkemedelsanvändning i öppna nät, till exempel Internet eller Sjunet, måste användarna vara identifierade och deras identitet säkerställd med en teknisk funktion som asymmetrisk kryptering (till exempel e-legitimation eller SITHS-certifikat), engångslösenord eller motsvarande. Dessutom ska personuppgifterna skyddas med kryptering vid själva överföringen. Syftet är att säkerställa att endast behöriga användare kan ta del av uppgifterna.

E-post och sms är exempel på överföringar som sker i öppna nät. Här är det särskilt viktigt att apoteket gör risk- och sårbarhetsanalyser eftersom ett apotek ofta hanterar integritetskänsliga uppgifter som rör recept, läkemedelsintag och rådgivning kring hälsa. Att införa tekniska begränsningar som minimerar de personuppgifter som skickas med oskyddad e-post och sms är en viktig del i integritetsskyddet. På www.datainspektionen.se/inbyggdintegritet går det att läsa mer om inbyggd integritet.

Personuppgiftsbiträde
Ett personuppgiftsbiträde är någon som behandlar personuppgifter för den personuppgiftsansvariges räkning. Ett exempel är om en tillståndshavare låter ett annat företag sköta hela eller delar av IT-driften. Skyddet för personuppgifterna får inte försämras om den personuppgiftsansvarige väljer att anlita ett biträde. Personuppgiftslagen innehåller därför regler som den personuppgiftsansvarige måste tänka på om man anlitar ett biträde.

Det ska finnas ett skriftligt avtal om biträdets behandling av personuppgifter för den personuppgiftsansvariges räkning. Avtalet ska reglera hur biträdet får behandla personuppgifterna och att denne är skyldig att vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas.

Tredjelandsöverföring
Ett tredjeland är ett land som inte är medlem i EU eller EES. Om apoteksinnehavaren anlitar ett företag i ett sådant land finns det finns särskilda regler om överföring av personuppgifter att tänka på. Läs mer om dessa på www.datainspektionen.se/tredjeland.

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

Datainspektionen