



Integriteten på den nya apoteksmarknaden

Information från Datainspektionen till apoteksmarknaden och till dig som är kund hos Apoteket

Den 1 juli 2009 upphörde Apoteket AB:s monopol på att sälja läkemedel. Nu kan olika företag öppna så kallade öppenvårdsapotek. De nya apoteken måste ha tillstånd från Läkemedelsverket för att få sälja och ge råd om läkemedel. Ett öppenvårdsapotek måste också ha ett säkert elektroniskt system för att hantera kund- och receptregister.

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

Information till dig som är kund hos Apoteket

Det centrala receptregistret

Tidigare var det Apoteket AB som hade ansvar för det centrala receptregistret och läkemedelsförteckningen men nu sköts detta av ett nybildat bolag: Apotekens Service AB. Precis som idag kommer din läkare eller sjuksköterska att sända receptet elektroniskt till det centrala receptregistret. Lagen om receptregister har nu fått ändrade och nya bestämmelser, exempelvis har den som arbetar inom Apotekens Service AB tystnadsplikt när det gäller hanteringen av uppgifter i receptregistret.

Vem på de nya apoteken får läsa recept?

När du vänder dig till ett öppenvårdsapotek för att hämta ut mediciner får behörig personal ta del av ditt recept i receptregistret. De får också ta del av dina läkemedels-

förmåner för att kunna räkna ut kostnaden. Öppenvårdsapoteket ska sedan skicka tillbaka uppgifter till receptregistret för att exempelvis landstingen ska faktureras på rätt sätt. När öppenvårdsapoteken hanterar dina personuppgifter ska de följa apoteksdatalagen, som är en helt ny lag som trädde i kraft den 1 juli 2009. På öppenvårdsapoteken har personal som har hand om läkemedel eller ger dig råd tystnadsplikt.

Hos öppenvårdsapoteken och Apotekens Service AB är det endast behöriga som får ta del av dina uppgifter och de får bara göra detta när det behövs i arbetet. Dessutom måste både öppenvårdsapoteken och Apotekens Service AB göra kontroller av registrens så kallade loggfiler för att se så att inga dataintrång eller onödiga inloggningar har gjorts.

Mer information

Mer information om din integritet på de nya apoteken hittar du på www.datainspektionen.se/apotek.

Information till apoteksmarknaden

Apoteksmarknaden och informations säkerheten

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

I och med omregleringen av apoteksmarknaden upphörde Apoteket AB:s monopol och ersätts 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 Apotekens Service AB. Läkemedelsverket har meddelat föreskrifter i frågor som rör apoteksmarknaden.

Apotekens Service AB och öppenvårdsapoteken får hantera känsliga personuppgifter enligt 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 men det finns också behov av andra säkerhetsåtgärder. Det är till exempel av största vikt att datakommunikationen skyddas under överföringen av personuppgifter mellan Apotekens Service AB och öppenvårdsapoteken. En oskyddad överföring av receptuppgifter innebär en avsevärd integritetsrisk.

Datainspektionens allmänna råd om säkerhet för personuppgifter ger vägledning om andra säkerhetsåtgärder som också måste vidtas. Råden hittar du på www.datainspektionen.se.



Information till anställda

En viktig del av integritetsskyddet är att användarna av ett IT-system får information om vikten av att följa gällande säkerhetsrutiner och att de får konkreta instruktioner om hanteringen av personuppgifterna.

Det är också lämpligt att informera anställda om tystnadsplikten så som den beskrivs i lagen om receptregister och lagen om yrkesverksamhet på hälso- och sjukvårdens område.

Information till de anställda om förutsättningarna för åtkomst och att loggkontroller utförs har en preventiv verkan och kan avhålla dem från att ta del av uppgifter när det inte behövs för att fullgöra arbetsuppgifterna.

Det är endast tillåtet att behandla personuppgifter om de registrerade för de ändamål som lagarna anger. Att ta del av recept och uppgifter om läkemedelsanvändning utan att behöva det för att utföra sina arbetsuppgifter är inte tillåtet. Den som olovligen bereder sig tillgång till uppgifter kan också göra sig skyldig till dataintrång.



Behörighetsstyrning

Lagarna anger att Apotekens Service AB 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 grupploggning 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. Så kallade sekretessmarkerade personuppgifter är normalt sett en typ av uppgift som kräver särskilda överväganden i analysarbetet.

Det ska finnas rutiner för behörighetsstyrningen för att kunna göra löpande ändringar och ta bort tilldelade behörigheter.

Åtkomstkontroll

Lagarna anger också att Apotekens Service AB 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. Kontrollerna ska göras systematiskt och fortlöpande vilket innebär att det inte räcker 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 bland annat riktar in sig på åtkomst till vissa

typer av uppgifter (till exempel sekretessmarkerade personuppgifter) eller åtkomst som sker utanför arbetstid.

Säkerhet vid överföring

Personuppgifter i recept eller om läkemedelsanvändning får överföras i öppna nät, till exempel Internet eller Sjunet, endast till identifierade användare vars identitet är 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 överföringen. Syftet är att säkerställa att endast behöriga användare kan ta del av uppgifterna. E-post är ett exempel på en överföring som oftast sker i öppet nät.

Personuppgiftsbiträde

Ett personuppgiftsbiträde (biträde) 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 försämrats om den personuppgiftsansvarige väljer att anlita ett biträde. Personuppgiftslagen innehåller regler som den personuppgiftsansvarige måste beakta om ett biträde anlitas.

Det ska finnas ett skriftligt avtal om bitrådets behandling av personuppgifter för den personuppgiftsansvariges räkning. I avtalet ska särskilt föreskrivas att biträdet får behandla personuppgifterna bara i enlighet med instruktioner från den personuppgiftsansvarige. Det ska också föreskrivas att biträdet är skyldigt att vidta tekniska och organisatoriska åtgärder enligt personuppgiftslagen.

Tredjelandsoverföring

Ett tredjeland är ett land som inte är medlem i EU eller EES. Det finns särskilda regler om tredjelandsoverföring av personuppgifter. Läs mer om tredjelandsoverföring på www.datainspektionen.se/tredjeland.

Mer information

Mer information om apoteksmarknaden och informationssäkerheten hittar du på www.datainspektionen.se/apotek.

Kontakta Datainspektionen

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

