Varför inte känsliga uppgifter via e-post?

Känsliga uppgifter enligt 13 § personuppgiftslagen får endast lämnas ut via öppna nät till identifierade användare vars identitet är säkerställd med en teknisk funktion som kryptering, engångslösenord eller motsvarande. Känsliga personuppgifter ska dessutom vid överföring via öppet nät, till exempel Internet, förses med krypteringsskydd.

Enligt Datainspektionen är även personnummer en känslig uppgift och skall också hanteras som sådan.

Det finns ett antal grundläggande säkerhetsbrister i de kommunikationsprotokoll som ligger till grund för e-postsystem. När ett e-postmeddelande skickas mellan olika e-postservrar över ett öppet nät passerar det andra servrar på vägen. Om informationen i e-postmeddelandet är okrypterad eller på annat sätt oskyddad finns det inget som hindrar att kopior av informationen sparas undan vid var och en av dessa servrar. Det finns dessutom inga möjligheter att utan extra åtgärder säkerställa att adressaten är den tänkta mottagaren.

Man kan då tycka att det skall vara ofarligt/säkert att skicka e-post internt inom landstinget, men e-postsystemet gör ingen skillnad om vi väljer en extern adress eller en intern. Risken att man väljer en felaktig adress och informationen hamnar utanför landstingets nät är stor och bara den risken är tillräcklig för att inte skicka känslig information via e-post.

Utöver risken att skicka till fel mottagare finns också andra problem, Enligt Patientdatalagen skall det finnas behörighetskontrollsystem i våra vårdsystem, detta för att säkerställa att endast de som behöver uppgifterna för sitt arbete kan ta del av dem. Om e-post med t ex patientuppgifter skickas internt mellan användare riskerar man att gå runt behörighetssystemen och uppgifter hamnar hos någon som inte har behörighet till dessa.

Vi är också skyldiga att i efterhand kunna kontrollera vem som tagit del av uppgifter i våra vårdsystem, detta görs genom att loggar sparas undan i en särskild loggdatabas som sedan kontrolleras via beställda kontroller eller stickprov.

Om information skickas via e-post till användare kan vi inte följa upp detta i efterhand på något sätt. Likaså om en patient har begärt att en viss vårdenhet skall spärras från att ta del av patientens uppgifter kan vi inte hantera det om uppgifter skickas via e-post mellan vårdenheter.

I vårt e-postsystem finns funktioner för att kunna skicka så kallad säker e-post, dvs att kunna säkerställa att mottagaren är den tänkta och att kryptera innehållet så att det är oläsligt förandra än mottagaren. För att kunna göra detta använder vi oss av våra e-tjänstekort vid sändning och mottagning.

Ett arbete kommer att påbörjas för att ta fram rutiner för hur man kan signera och kryptera e-post.

Med hjälp av säker e-post är det ändå inte fritt fram att skicka patientuppgifter mellan

användare, vi förhindrar åtminstone att uppgifterna kan läsas om de hamnar hos fel användare utanför landstinget. Men risken att man kringgår behörighetssystem, loggfunktioner och spärrhantering är ändå stor.

För att kunna skicka känsliga uppgifter med säker e-post måste detaljerade riktlinjer tas fram som visar tydligt vad man får och inte får göra.

E-post, säker eller ej får heller inte bli en ersättare för remiss och svarshanteringen inom vårdsystemen, den hanteringen måste skötas via därför framtagna system.

E-post mellan vårdgivare och allmänhet/patienter
Utöver det som tagits upp när det gäller säkerhetsbrister med e-post är som tidigare nämnts är problemet att veta om mottagaren är den tänkta. En e-postadress är enkel att förfalska och därför kan man inte med säkerhet veta vem som skickat ett e-postmeddelande.

E-tjänsten "Mina vårdkontakter" uppfyller de krav på säkerhet och sekretess som ställs eftersom inloggning kan ske med e-legitimation för allmänhet/patient, och på vårdgivarsidan kan man endast logga in med e-tjänstekort.