

Säker inloggning i IT-system inom vård och omsorg

Rekommendation till Famnas medlemmar

Det pågår ett intensivt arbete med att skapa förutsättningar för alla vård- och omsorgsgivare att säkert kunna logga in i och överföra information mellan olika IT-system. Enligt de lagstadgade kraven (t.ex. patientdatalagen) och information från Datainspektionen räcker det inte att logga in i system som hanterar känslig personinformation med bara användarnamn och lösenord. Detta måste hanteras med så kallade tvåfaktorsinloggnings, där man kombinerar smarta kort, SMS, eller andra certifikatbärare med personliga lösenord. Detta kan jämföras med e-legitimation som används av många banker eller Skatteverket. En viktig förutsättning är också att man vid utlämnande av certifikatbärare (smarta kort) har rutiner som säkerställer att det är rätt person som använder rätt kort i rätt roll och för rätt uppdrag.

Det är med andra ord komplexa frågeställningar inte minst när det handlar om olika utförare och olika beställare som alla är olika juridiska huvudmän. Famnas IT-nätverk har de senaste veckorna intensivt jobbat med att försöka få svar på en del av frågorna och sammanfattar frågorna här:

HSA/SITHS-kort eller andra smarta kort?

HSA/SITHS är en kombination av ett register där man definierar en persons uppdrag inom vården och omsorgen och ett certifikat för att säkerställa att det är rätt person som använder kortet. HSA/SITHS har varit den lösningen som de flesta landsting använder idag och övriga är på väg att införa HSA/SITHS. Under den senaste tiden har den också blivit huvudlösningen för de flesta kommunerna. Det finns även andra lösningar för tvåfaktorsinloggning, t.ex. Skatteverkets ID-kort, men de är inte tjänstekort utan personliga kort. HSA/SITHS är standarden för flera av de nationella tjänster som i början av 2012 kommer kräva säkra inloggnings och är den lösning som de flesta landsting och kommuner kommer att välja.

Famna rekommenderar därför sina medlemmar att satsa på HSA/SITHS när man införskaffar lösningar för säker inloggning.

Tjänster och system som använder HSA/SITHS

Redan idag kan man använda inloggning med SITHS-kort i t.ex. Senior alert och Palliativregistret samt ett flertal andra kvalitetsregister. Från mitten av januari kommer Webcare (Systemet för samordnad vårdplanering i Stockholms län) att kräva HSA/SITHS för inloggning och i mitten av mars kommer dosordination av läkemedel (nuvarande Apodos) kräva HSA/ SITHS. Det är att räkna med att i framtiden även journal- och sociala dokumentationssystem kräver tvåfaktorsinloggning.

Hur gör jag för att skaffa säkra kort?

Tillgången till HSA och SITHS varierar i landet. De flesta landsting tillhandahåller HSA och SITHS till sina privata vårdcentraler, i flera fall också till övriga privata vårdgivare med avtal. Detta innebär att de medlemmarna som bedriver hälso- och sjukvård med landstingsavtal

borde lätt kunna få tillgång till HSA/SITHS. För medlemmar som endast bedriver verksamhet med avtal med kommuner blir det svårare. Det finns många kommuner som erbjuder sina utförare HSA/SITHS i samarbete med respektive landsting. Det finns dock vissa kommuner som inte har bestämt sig hur man ska hantera detta i sina egna system och där man inte är i behov av HSA/SITHS. Här kan det finnas problem för mindre aktörer att få hjälp av kommunen. Famna jobbar just nu bl.a. med SKL och Kommunförbundet i Stockholms län för att hitta lösningar.

Som första steg rekommenderar Famna sina medlemmar att vända sig till sin beställare (landsting eller kommun) för att diskutera hur man kan få tillgång till HSA/SITHS. Ni som inte har börjat denna kontakt bör göra det omgående.

Om kommunen inte hjälper till kan man vända sig till Svensk e-identitet AB, ett företag i Uppsala som tillhandahåller HSA/SITHS till bl.a. privata utförare som är godkänd som HSA-ombud av Inera AB som förvaltar HSA nationellt. Hursomhelst meddela detta till oss för att vi kan få en bild om hur situationen är.

Behöver ni hjälp med dessa frågor hör gärna av er.

För Famnas IT-nätverk
Thomas Schneider, 0708-108157
thomas.schneider@famna.org