inera

Rekommendationer kring skyddade personuppgifter inom HSA och SITHS

Version 2.1.2, 2016-12-30

Innehåll

Revisionshistorik

Version	Datum	Kommentar
1.0	2010-12-07	Första fastställda version
2.0	2014-10-21	Uppdaterat utifrån gällande rutiner och med förtydligande av ansvar för arbetsgivaren.
2.1	2015-06-09	Tillagd hänvisning till dokumentet ”Tjänster med åtkomst till skyddade personuppgifter från HSA” samt förtydligande i bilaga 1 om vad synliggörande av uppgifter innebär för en person med skyddade personuppgifter. Fastställd av HSA Förvaltningsgrupp.
2.1.1	2016-03-24	Mindre språklig justering.
2.1.2	2016-12-30	Justerat efter ändrad benämning på HSA-policytillämpning (från HPTA resp. HPTB till HPT Producent resp. HPT Konsument).

1 Inledning

1.1 Skyddade personuppgifter

Skyddade personuppgifter är Skatteverkets samlingsrubrik för skyddsåtgärderna sekretessmarkering, kvarskrivning och fingerade personuppgifter inom folkbokföringen. Mer information om dessa skyddsåtgärder finns på www.skatteverket.se/folkbokforing [1].

Personuppgifter, inklusive sekretessmarkering, aviseras från Skatteverket till andra myndigheter. Mottagande myndighet avgör sedan hur den ska hantera skyddade personuppgifter i sina system.

1.2 Vikten av säkerställd identitet

För att en person ska kunna arbeta i ett vård- och omsorgssystem krävs att personens identitet är säkerställd. Säker identifiering av personal möjliggörs genom att personen finns upplagd i HSA, har ett HSA-id och en elektronisk tjänstelegitimation, ett HCC. För att få ett HSA-id och HCC krävs att personen kan styrka sin identitet.

HSA-policyn [2] beskriver att skyddade personuppgifter inte får finnas synliga i HSA utan personens medgivande och ställer krav på att anslutna organisationer redovisar hur nytillkomna skyddade personuppgifter döljs i HSA. För att få ett HCC krävs att den anställde finns i HSA.

2 Rekommendationer

Följande rekommendationer ges kring hanteringen av personer med skyddade personuppgifter inom HSA och SITHS:

2.1 Person med skyddade personuppgifter ska av arbetsgivaren informeras om hur uppgifterna hanteras

Berörd organisation (arbetsgivaren) ansvarar för att informera personer med skyddade personuppgifter, dels om hur uppgifterna används inom HSA och SITHS dels om vem som har tillgång till uppgifterna.

2.2 Begränsad användning av informationen

Endast av HSA Förvaltningsgrupp godkända tjänster får ta emot uppgifter om personer med skyddade personuppgifter och dessa system får endast tillgång till de uppgifter som är nödvändiga. Uppgifter från HSA om personer med skyddade personuppgifter lämnas i normalfallet endast ut till tjänster i samband med att en person med skyddade personuppgifter själv väljer att logga in med stark autentisering i den aktuella tjänsten (t.ex. via SITHS-kort.)

I de fall informationen vidareförmedlas till andra system ska skyddet framgå även i dessa system.

De tjänster/brukarorganisationer som får tillgång till uppgifter om personer med skyddade personuppgifter ska i sin HPT Konsument (HSA-policytillämpning för konsumerande organisation) beskriva hur dessa uppgifter hanteras. För mer information om respektive tjänsts

hantering av skyddade personuppgifter se dokumentet ”Tjänster med åtkomst till skyddade personuppgifter från HSA” [3].

2.3 Kontroll mot befolkningsregistret ska ske

Skyddade personuppgifter kontrolleras mot befolkningsregistret vid registrering av personer i HSA. Verifiering av att en person fortfarande har skyddade personuppgifter eller identifiering av personer som nyligen har fått sina personuppgifter skyddade sker via den obligatoriska slagningen mot Skatteverket i HSA som varje organisation genomför månatligen.

2.4 Särskild hantering i HSA

Person med skyddade personuppgifter måste finnas i HSA för att uppfylla kravet på säker identifiering av vårdpersonal i vårdinformationssystem. Personen kan dock själv välja om uppgifterna ska vara synliga eller dolda i HSA. Om personen inte begär att uppgifterna ska vara synliga är utgångsläget alltid att uppgifterna ska vara dolda.

Personer med skyddade personuppgifter markeras i HSA genom ifyllnad av attributet "skyddad person" (*hsaProtectedPerson*) samt att personposten blir kopplad till objektklassen "*hsaConfidentialPerson*" som gör att personposten döljs. Om personen vill vara synlig i HSA tas denna objektklass bort och personen blir synlig som alla andra. Attributet "skyddad person" behålls alltid så länge personen har skyddade uppgifter. Rutin för denna hantering ska finnas i den lokala organisationen.

För att begränsa åtkomsten till skyddade personuppgifter har endast ett fåtal administratörer tillgång till uppgifterna. Administratörerna ska ha goda kunskaper om hur personer med skyddade uppgifter ska hanteras. Regelbunden uppföljning av åtkomst till dessa uppgifter bör göras. I HSA Admin är det endast rollerna Huvudadministratör och Centraladministratör som kan hantera poster för personer med skyddade personuppgifter.

Rutin för att hantera personer med skyddade personuppgifter i HSA Admin beskrivs i HSA Admin Handbok som finns på www.inera.se.

2.5 Särskild hantering i SITHS

I SITHS kan personer med attributet "skyddad person" (*hsaProtectedPerson*) ifyllt endast hanteras av administratörsrollen KUR (CRA med ansvar för personer med skyddade personuppgifter).[1]

För att säkerställa att SITHS-kort till personer med skyddade personer endast levereras till KUR-behörig korthandläggare måste ett särskilt kortkontor registreras hos kortleverantören.

Alla sökningar som görs på personer med skyddade personuppgifter loggas och kan följas upp i efterhand i SITHS Admin. Rutin för kortutgivning till personer med skyddade personuppgifter finns på www.siths.se [4].

[1] Inom SITHS hanteras alla personer med skyddade personuppgifter på samma sätt, oavsett om de valt att vara synliga eller inte. SITHS Admin tar alltså inte hänsyn till om personposten är dold eller inte i HSA, d.v.s. om posten är kopplad till objektklassen "*hsaConfidentialPerson”*.

2.5.1 SITHS-korttyper till personer med skyddade personuppgifter

Det finns särskilda korttyper framtagna för personer med skyddade personuppgifter. Dessa korttyper ser likadana ut som de ordinarie korttyperna men hanteringen av dessa kort är begränsad. Pinkoder till kort som ska ges ut till personer med skyddade personuppgifter levereras till personen via Skatteverkets förmedlingskontor. Detta till skillnad mot ordinarie korttyper där pinkoder skickas till folkbokföringsadressen.

Personer med skyddade personuppgifter kan sedan 2014 även få reservkort.

3 Referenser

Nr	Referens
[1]	Skatteverkets vägledning för hantering av sekretessmarkerade personuppgifter i offentlig förvaltning. www.skatteverket.se/folkbokforing.
[2]	HSA Policy. Se www.inera.se/hsa under Dokument och Styrande
[3]	Tjänster med åtkomst till skyddade personuppgifter från HSA. Se www.inera.se/hsa
[4]	Rutin för kortutgivning till person med skyddade personuppgifter. Rutin för kortutgivning med skyddade personuppgifter. Se www.inera.se/siths under Regelverk och Regler, rutiner, processer

Bilaga 1 Information om HSA till personal med skyddade personuppgifter

Nedan presenteras ett förslag på information om HSA till personal med skyddade personuppgifter. Informationstexten kan användas i sin helhet eller kompletteras med egen lokal information. Notera att det är arbetsgivarens ansvar att informera berörda personer.

Till dig som har skyddade personuppgifter och som arbetar i <*organisationens namn*>

Som anställd inom vård och omsorg finns du registrerad i en gemensam katalog för vårdanställda i Sverige, Katalogtjänst HSA. Uppgifterna om dig hämtas oftast från en lokal katalog i den organisation där du har din anställning.

Både HSA-katalogen och lokala kataloger är att betrakta som publika kataloger, där den anställdes arbetsplats- och yrkesuppgifter exponeras nationellt. Om du arbetar i e-tjänster/system som är anslutna till HSA-katalogen eller den lokala katalogen blir dina uppgifter synliga också i dessa. För en förteckning över vilka nationella e-tjänster som hämtar information om personer med skyddade personuppgifter hänvisas till www.inera.se/hsa under Dokument och Stödjande. För motsvarande förteckning för den lokala användningen hänvisas till <*ange plats här*>.

Arbetsgivaren ska hantera dina personuppgifter i sina system på ett skyddsvärt sätt. I HSA-katalogen är standard att den som har skyddade personuppgifter inte visas vid sökningar och att uppgifterna endast hanteras av särskilda katalogadministratörer. Du väljer själv om du vill vara synlig vid sökningar, men ansvarar då också för de konsekvenser detta kan medföra om dina uppgifter exponeras. *Observera att ett synliggörande i HSA innebär att registrerad information om dig vid efterfrågan kan exporteras till alla HSA-anslutna tjänster som begär detta. Vidare erhåller dessa tjänster då ingen information om att du har skyddade personuppgifter.* Godkännande av att synliggöra dina uppgifter lämnar du skriftligen till <*ange rutin och anmälningsväg*>.

Om du i ditt arbete utför aktiviteter i system som innehåller patientinformation loggas dina uppgifter som användare i systemen oavsett om du valt att synliggöra dina uppgifter eller inte. Om patient begär loggutdrag från elektronisk journal i offentlig hälso- och sjukvård ska du vara medveten om att din arbetsgivare måste lämna ut din användaridentitet.

Har du flera frågor kontakta <*ange lämplig person, t.ex. HR-ansvarig*>.