



Livscykelhantering av personuppgifter i HSA

Innehåll

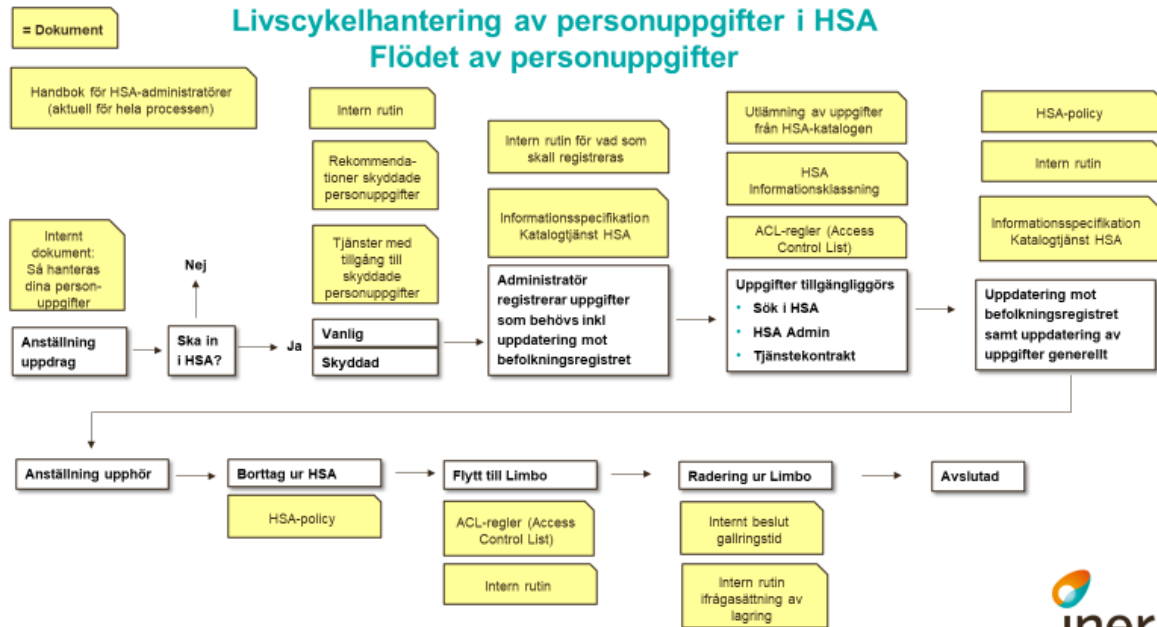
Livscykelhantering av personuppgifter i HSA.....	1
Flödet av personuppgifter i HSA	2
Förändringar i HSA kopplat till HSA-schema och teknik	3
Dokument som säkerställer den personliga integriteten i HSA.....	4

Revisionshistorik		
Version, datum	Författare	Kommentar
1.0, 2018-05-23	Anna Lettse	Fastställd i version 1.0
1.1, 2021-08-23	Henrika Littorin	Generell översyn och uppdatering i enlighet med HSA Internrevision 2021

I detta dokument beskrivs hur livscykelhanteringen av personuppgifter i HSA fungerar och vilka regelverk och dokument som finns för att säkerställa den personliga integriteten genom dessa processer.



Flödet av personuppgifter i HSA

1. En person registreras i HSA av behörig administratör

- 1.1. En person anställs eller får ett uppdrag för Inera eller en HSA-ansluten organisation. Personen tecknar ett anställnings- eller uppdragsavtal.
- 1.2. Personen behöver få åtkomst till olika system och applikationer och registreras då i HSA. Personens personuppgifter och anställningsrelaterade uppgifter kontrolleras mot interna och externa källor, och registreras i HSA av utsedd HSA-administratör. Exempel på interna och externa källor är personalsystem och Skatteverkets folkbokföringsregister. Registrering av uppgifterna hanteras enligt HSA:s regelverk och rutiner, där särskild hantering gäller för personer med skyddade personuppgifter.
- 1.3. Personuppgifterna i HSA kompletteras med den information som organisationen behöver om personen, t.ex. legitimerad yrkesgrupp enligt HOSP, e-postadress samt anställningstitel.
- 1.4. Personen tilldelas aktuella behörigheter i HSA, bl.a. medarbetaruppdrag, vilket innebär åtkomst till andra system, både lokala och nationella.

En persons uppgifter i HSA uppdateras av behörig administratör:

- 1.5. Om personen byter namn (t.ex. då personen gifter sig eller skiljer sig) eller person-id (t.ex. att ett samordningsnummer ändras till personnummer) så uppdateras uppgifterna genom slagning mot folkbokföringsregistret. Detsamma gäller om personen får skyddade personuppgifter eller om personen slutar att ha skyddade personuppgifter. Frekvensen av kontrollen styrs genom HSA-policy.
- 1.6. Om personen får ny eller ändrad yrkeslegitimation ändras detta efter uppdatering mot HOSP-registret. Frekvensen av kontrollen styrs genom HSA-policy.
- 1.7. Om personen får ändrade anställningsuppgifter och nya, förändrade uppdrag ändras information om titel samt uppdrag utifrån information från chefer eller personalsystem i den egna organisationen. Frekvensen av kontrollen styrs genom HSA-policy.
- 1.8. Även registrerade kontaktuppgifter uppdateras vid behov.



2. En persons uppgifter i HSA arkiveras och raderas:

- 2.1. När en person slutar sin anställning eller sitt uppdrag i organisationen rensas information om den registrerade i HSA så att endast ett fåtal uppgifter, särskilt person-id och HSA-id, finns kvar. De kvarvarande uppgifterna flyttas till Limbo, en särskild dold arkiveringsplats i HSA. Där lagras uppgifterna i enlighet med HSA-policyn.
- 2.2. Efter en specificerad arkiveringstid, som beslutas av respektive organisation, raderas personuppgifterna från Limbo i enlighet med HSA-policyn och rensningsrutiner. Arkiveringstiden kan variera, men är oftast minst fem år (preskriptionstiden för dataintrång).
- 2.3. En person som slutat sin anställning kan också begära radering av uppgifterna innan arkiveringstidens slut. En prövning görs då för att avgöra om det är möjligt att radera uppgifterna. I denna prövning tittar organisationen bland annat på om personen haft behörigheter för åtkomst till patientuppgifter eller haft administratörsbehörigheter i HSA.

Förändringar i HSA kopplat till HSA-schema och teknik

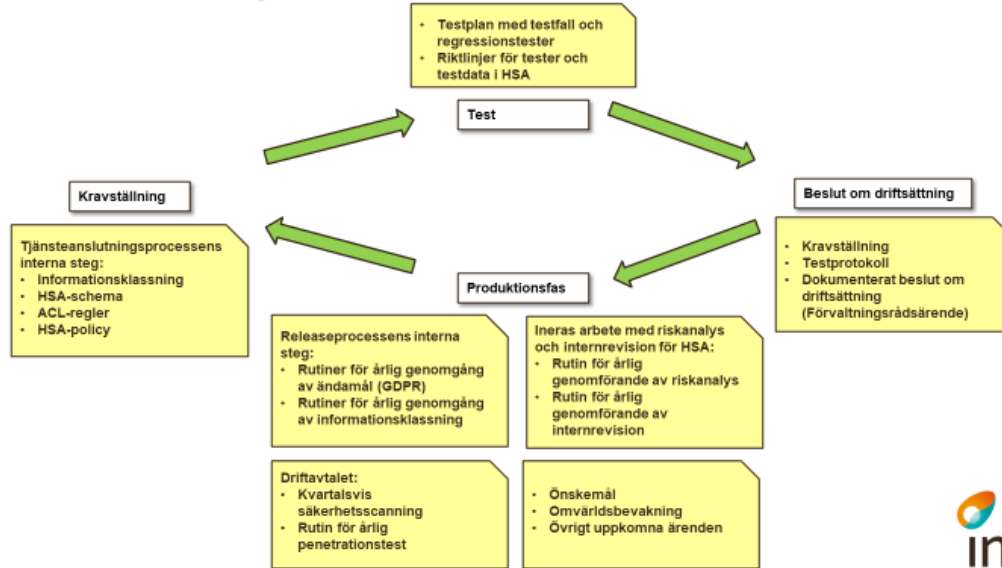
HSA som system förändras kontinuerligt genom schemaändringar. Schemaändringarna innebär bland annat tillägg och borttag av information som är möjlig att registrera i tjänsten. Önskemål om tillägg och borttag kommer in både från anslutna producenter (oftast vårdgivare) och konsumenter (tjänster). Ändringsbehov kan även komma från årliga revisioner och riskanalyser samt genomförd säkerhetsscanning och penetrationstest.

Inför varje schemaförändring sker en analys av om de egenskaper som föreslås läggas till i systemet verkligen behövs. Om egenskaperna som ska läggas till är personuppgifter diskuteras och beslutas även om särskilda skyddsåtgärder behöver vidtas för att skydda informationen (så kallad informationsklassning). Varje år görs även en total översyn av informationsklassningen för HSA för att identifiera eventuellt behov av förändringar i skyddsbehov för informationen.

Varje schemaförändring testas noggrant, även ur informationssäkerhetsperspektivet. Riktlinjer för tester och testdata i HSA föreskriver bland annat att inga skarpa persondata ska användas i testsyfte samt att tester ska genomföras i testmiljö innan produktionssättning.



Livscykelhantering av personuppgifter i HSA Förändringar i HSA kopplade till HSA-schema och teknik



Dokument som säkerställer den personliga integriteten i HSA

Nedan presenteras de policys, riktlinjer, avtal, rekommendationer och beskrivningar som säkerställer den personliga integriteten under hela HSA:s livscykel:

Nationella styrande dokument (policy, avtal och riktlinjer):

- HSA-policy
 - Anslutna organisationer förbinder sig att följa denna genom HSA Anslutningsavtal med tillhörande HPT (HSA-policytillämpning)
- Riktlinjer för tester och testdata i HSA
- Informationsspecifikation Katalogtjänst HSA
- Informationsklassning för HSA
- ACL-regler (tekniska regler för vilken användare som kommer åt vilken information)

Nationella stödjande dokument (beskrivningar, rekommendationer):

- Handbok för HSA-administratörer
- Utlämning av uppgifter från HSA-katalogen
- Rekommendationer kring skyddade personuppgifter HSA SITHS
- Schemauppdateringsprocess (finns även ett internt dokument, Releaseprocessens interna steg, som säkerställer korrekt hantering)
- Tjänsteanslutningsprocess (finns även ett internt dokument, Tjänsteanslutningsprocessens interna steg, som säkerställer korrekt hantering)

Interna rutiner för respektive ansluten organisation