HSA-policy

inera

Innehåll

Kontaktuppgifter

Denna policy förvaltas av Inera AB. Frågor, synpunkter och förslag rörande policyn skickas till:

Organisation: Inera AB
Box: 17703
Postnummer: 118 93
Ort: Stockholm
E-post: kundservice@inera.se
Webbplats: www.inera.se

Revisionshistorik

Version	Datum	Kommentar
4.1	2018-03-13	**HSA-policy version 4.1 fastställdes av HSA Policygrupp den 13 mars 2018 och träder i kraft den 25 maj 2018.** Referenser till Personuppgiftslagen (PuL) har ersatts med referenser till EU:s dataskyddsförordning (GDPR). Kravet på lagring av förhållandet personidentitet/HSA-id har ändrats från minst 10 år till att respektive ansluten producerande organisation själv ska besluta om arkiveringstid med hänsyn till gällande lagstiftning. Krav på hantering av loggar har ändrats så att förändringar av HSA-information som lagras nationellt sparas i fem år samt att ansluten producerande organisation med egen intern katalog måste fatta motsvarande beslut för den egna organisationens loggar. Anslutningsformen HPT Fingerad data har tagits bort. Förtydligande har gjorts av att krav för HSA-ombud gäller såväl producerande som konsumerande organisationer. HSA Förvaltningsgrupp har ersatts av HSA Policygrupp efter Ineras nya ramverk. Beskrivning av att kommunikation med interna källsystem hos producerande organisationer med fullständig anslutning får ske okrypterat under vissa förutsättningar har lagts till. Krav på att personer med skyddade personuppgifter ska erbjudas möjlighet att välja om uppgifterna ska göras synliga är ändrat från ska till bör. Förtydligande har gjorts att tidigare person-id inte bör lagras, inte ens i Limbo eller motsvarande struktur för inaktiva personer, då en person byter personidentitet (t.ex. från samordningsnummer till personnummer). Kontroll av uppdragsförhållande för studenter tillåts göras terminsvis istället för kvartalsvis för de producerande organisationer som beskriver detta i sin HPT Producent. Hänvisning till SOSFS 2008:14 är borttagen (ersattes 1 mars 2017 av HSLF-FS 2016:40). Referenser till MSB:s föreskrifter och ISO-standarden 27002 är justerade. Malldokumenten för fullständig anslutning har fått förtydligade namn – ”HPT Producent, fullständig” resp. ”HPT Konsument, fullständig”. I bilaga 2 i HPT Producent, fullständig, har redovisning av synkronisering från/till lokal katalog brutits ut i särskilt avsnitt. Mindre språkliga justeringar i samtliga dokument.

Sammanfattning – Executive summary

HSA är en nationell katalogtjänst för organisationer verksamma inom vård och omsorg. Katalogtjänsten är främst anpassad för vård- och omsorgsverksamhet men kan även användas av andra verksamheter inom dessa organisationer.

HSA regleras av en nationell policy och tillhörande styrande dokument. Organisationer verksamma inom vård och omsorg kan välja att ansluta till HSA och ansvarar då för att samtliga krav i policyn efterlevs.

Anslutna organisationer kan utgöra producenter och/eller konsumenter av HSA-information. Varje ansluten organisation tar fram och förvaltar en HSA-policytillämpning (HPT) som beskriver hur organisationen uppfyller HSA-policyn.

Informationen i HSA ägs och förvaltas av respektive ansluten producent. För drift, ändringshantering och förvaltning av teknisk plattform svarar Inera AB.

De krav som ställs på producenter av HSA-information är bland annat:

- Att en HSA-ansvarig utses som praktiskt ansvarar för organisationens anslutning
- Att informationen i HSA ska följa vid var tid gällande schema och värdemängder
- Att informationen ska förvaltas så att innehållet är uppdaterat och korrekt
- Att internrevision av efterlevnad till HSA-policyn görs minst en gång per år
- Vid uppdatering av HSA från lokal katalog eller motsvarande även att konfidentialitet, riktighet, tillgänglighet och spårbarhet säkerställs i den lokala tjänsten

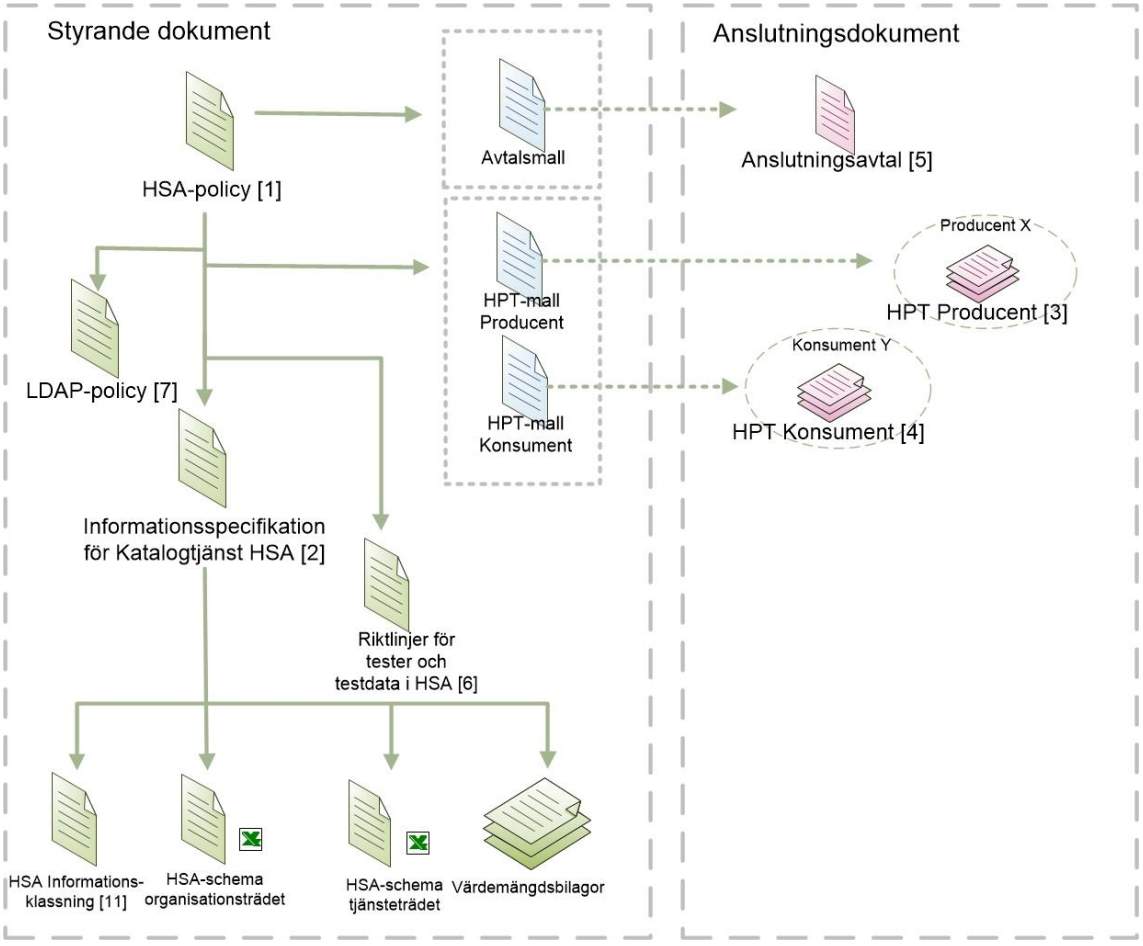
De krav som ställs på konsumenter av HSA-information är bland annat:

- Att en kontaktperson utses som praktiskt ansvarar för organisationens anslutning
- Att informationen från HSA endast får användas på det sätt som är beskrivet i HPT godkänd av HSA Policygrupp
- Att internrevision av efterlevnad till HSA-policyn görs minst en gång per år
- Att kontinuitetsplanering finns för den händelse att HSA ej är tillgänglig
- Att om konsument lagrar HSA-information i den egna tjänsten måste informationen hållas uppdaterad över tid och den får inte ändras på annat sätt

HSA Policygrupp, som består av representanter för informationsägarna, fattar beslut om ändringar i HSA-policyn samt godkänner nya och förändrade anslutningar till HSA av såväl producenter som konsumenter. Inera AB har inte rätt att lämna ut information från HSA annat än på informationsägarnas uttryckliga begäran.

Övergripande dokumentstruktur för HSA

Styrning och användning av HSA regleras i ett antal dokument. Bilden nedan visar den övergripande dokumentstrukturen för HSA och de inbördes relationerna mellan dokumenten.



Den övergripande dokumentstrukturen består av:

- **HSA-policy [1]** (detta dokument), ett styrande dokument för HSA på övergripande nivå.
- **Informationsspecifikation för Katalogtjänst HSA [2]**, beskriver informationsinnehållet i HSA. Till detta dokument finns följande bilagor:
    - HSA Informationsklassning [11], som beskriver klassning av HSA-informationen ur konfidentialitets-, riktighets-, tillgänglighets- och spårbarhetssynpunkt
    - HSA-schema, organisationsträdet
    - HSA-schema, tjänsteträdet
    - Värdemängdsbilagor, som beskriver tillåtna värden för vissa attribut

- **HSA-policytillämpning (HPT) för producent [3]**, skrivs av varje organisation som publicerar information till HSA och beskriver hur den enskilda organisationen uppfyller kraven i HSA-policyn. Det finns en särskild variant av HPT som är framtagen för de organisationer som endast använder det nationellt förvaltade administrationsgränssnittet HSA Admin för att uppdatera information i HSA manuellt.
- **HSA-policytillämpning (HPT) för konsument [4]**, skrivs av organisationer som använder information från HSA såsom konsument och beskriver hur organisationen uppfyller kraven på informationshantering i HSA-policyn. Det finns en särskild variant av HPT som är framtagen för de organisationer som endast hämtar publik enhetsinformation.
- **Anslutningsavtal [5]**, tecknas mellan Inera AB och producenten respektive konsumenten och reglerar ansvarsfördelningen mellan parterna.
- **Riktlinjer för tester och testdata i HSA [6]**, beskriver hur tester och testdata hanteras samt vilka regler som gäller för registrering och hantering av fingerade uppgifter.
- **LDAP-policy [7]** beskriver hur kommunikation via LDAP ska ske mot HSA.

1. Introduktion

1.1 Översikt

Detta dokument utgör en nationell policy för HSA. Policyn reglerar etablering, drift och förvaltning av katalog eller motsvarande innehållande enheter, funktioner, personal och tjänster huvudsakligen inom vård och omsorg enligt HSA-modellen. Efterlevnad av denna policy är en förutsättning för att vara ansluten till HSA.

Policyn förvaltas och fastställs av HSA Policygrupp.

Direktanslutna organisationer, såväl producerande organisationer (producenter) som konsumerande organisationer (konsumenter), bekräftar efterlevnad av denna policy genom anslutningsavtal och upprättande av en HSA-policytillämpning (HPT), som godkänns av HSA Policygrupp.

1.2 Begrepp och definitioner

Definitioner av begrepp som används i denna policy finns i särskilt dokument [8].

Tvingande krav för anslutna producenter och konsumenter anges i denna policy med verben och fraserna **ska**, **ska ej**, **får** och **får ej** i fet stil. De delar som är rekommendationer anges med verben och fraserna **bör**, **kan** och **bör ej** i fet stil.

1.3 Syfte med HSA och HSA-policyn

Syftet med HSA är att samla kvalitetssäkrad information om organisation och medarbetare inom organisationer verksamma inom vård och omsorg. Katalogtjänsten är främst anpassad för vård- och omsorgsverksamhet men kan även användas av andra verksamheter inom dessa organisationer. Samlad information gör det möjligt att upprätthålla god kvalitet på uppgifterna, minska dubbeladministration, samt att underlätta åtkomsten till informationen för andra e-tjänster.

Innehållet i HSA omfattar – men är inte begränsat till – förutsättningar för utfärdande av elektroniska identiteter, behörighetsgrundande information och underlag för vårdsökning.

Syftet med HSA-policyn är att säkerställa att konsumenter av informationen kan känna sig trygga med att informationen de får ta del av är korrekt och aktuell över tid samt att producenter av HSA-information kan känna sig trygga med att deras information används på ett ansvarsfullt sätt.

1.4 Målgrupp och tillämplighet

Målgrupper för denna policy, utöver HSA Policygrupp, är HSA-ansvariga och beslutsfattare hos anslutna producerande organisationer samt kontaktpersoner och beslutsfattare hos anslutna konsumerande organisationer.

Policyn är tillämpbar för etablering, drift och förvaltning av HSA samt för användning av information från HSA.

2 Allmänna förutsättningar

Med ”producerande organisation” och synonymen ”producent” avses organisation inom HSA som tillgängliggör information från den egna organisationen. Begreppet omfattar således både direktansluten och tredjepartsansluten producent. En producent har rätten att, med iakttagande av befintligt regelverk, konsumera information från andra anslutna producenter.

Med ”direktansluten producent” avses organisation som har eget HSA-avtal med Inera.

Det finns två anslutningsformer för ”direktansluten producent”, fullständig eller förenklad. Den senare innebär att producenten bara kan administrera och läsa information via HSA Admin. Att hämta och nyttja information från HSA via t.ex. tjänstekontrakt är bara tillåtet vid fullständig anslutning.

Med ”konsumerande organisation” och synonymen ”konsument” avses organisation eller tjänst som nyttjar information från HSA utan att egen information tillgängliggörs i HSA.

Det finns två anslutningsformer för konsument, fullständig eller förenklad. Den senare innebär att konsumenten bara får läsa publik enhets- och funktionsinformation enligt särskild specifikation.

Med ”HSA-ombud” avses direktansluten organisation som

- med medgivande från eller på uppdrag av en annan producerande organisation (tredjepartsansluten) ansvarar för att tillgängliggöra och vid behov registrera den andra organisationens information i HSA. Detta gäller oavsett var informationen placeras i HSA.
- alternativt på uppdrag av en annan konsumerande organisation/tjänst (tredjepartansluten) ansvarar för att tillhandahålla information från HSA.

2.1 Ansvarsförhållanden

För varje direktansluten producent **ska** det finnas en huvudansvarig för anslutningen till HSA, kallad HSA-ansvarig.

Alla kontakter rörande HSA-frågor kommer att gå till den HSA-ansvarige som **ska** ha tillräckliga mandat och kontaktvägar inom sin organisation för att kunna hantera dessa frågor.

Direktansluten producent **ska** utse en ställföreträdande HSA-ansvarig som kan täcka upp för HSA-ansvarig under kortare frånvaro (t.ex. semester). HSA-ansvarig **bör** anmäla ställföreträdande HSA-ansvarig till HSA Förvaltning för att denna person ska ges samma rättigheter som HSA-ansvarig.

HSA-ombud **ska** reglera informationsägarskap och informationssäkerhetsansvar med sina tredjepartsanslutna organisationer.

För varje konsument **ska** det finnas en utsedd kontaktperson som ansvarar för konsumentens användning av information från HSA och kontakter gentemot HSA.

2.2 Förpliktelser för producerande organisation

2.2.1 Allmänt

Ansluten producent **ska** arbeta enligt denna policy och garantera att organisationen till fullo uppfyller samtliga policykrav.

2.2.2 Förpliktelser för HSA-ansvarig hos direktansluten producerande organisation

En förutsättning för att inneha rollen som HSA-ansvarig är att personen genomgått en av Inera godkänd grundutbildning för HSA.

Den HSA-ansvarige **ska** tillse att:

- organisationens uppgifter i HSA är aktuella och korrekta så att andra anslutna organisationer kan förlita sig på uppgifternas riktighet
- behandling av personuppgifter i HSA följer EU:s dataskyddsförordning (GDPR)
- en organisation för administration av information i HSA upprättas, bemannas och dokumenteras
- organisationen har en tillgänglig och bemannad funktion som tar emot drift- och störningsinformation från HSA:s driftorganisation
- regelbunden internrevision sker rörande efterlevnad av HSA-policyn
- det finns en kontinuitetsplan (avbrotts- och katastrofplan)
- det finns ett dokumenterat regelverk för hur administratörer utses och för hur behörigheter tilldelas
- information från HSA Förvaltning sprids inom organisationen inklusive eventuella tredjepartsanslutna producerande organisationer
- LDAP-policyn för HSA [7] följs
- Riktlinjer för tester och testdata i HSA [6] följs
- personer med rättigheter att administrera organisationens HSA-information har kännedom om och arbetar i enlighet med HSA-policyn och HPT
- aktuella kontaktuppgifter till HSA-ansvarig och ställföreträdande HSA-ansvarig finns registrerade i HSA
- hålla sig informerad om vad som händer inom HSA genom att till exempel läsa nyhetsbrev och delta vid nätverksmöten.

Om information i HSA uppdateras från en lokal katalog eller motsvarande **ska** HSA-ansvarig ansvara för:

- användning och säkerhet i den lokala katalogen eller motsvarande vid utveckling, anskaffning, drift och förvaltning
- driftgodkännande av anslutning till HSA.

2.2.3 HSA-policytillämpning för producent (HPT Producent)

Direktansluten producent **ska** ta fram ett särskilt dokument, ”HSA-policytillämpning för producent” (HPT Producent), som beskriver hur denna policy tillämpas. Framtagen HPT **ska** godkännas av HSA Policygrupp.

HPT **ska** utformas enligt anvisningarna i dokumentet ”Mall för HSA-policytillämpning för producent” [3]. All användning av HSA **ska** dokumenteras i HPT.

Godkänd HPT **ska** arkiveras av direktansluten producent. Namn på organisation som har godkänd HPT kommer att publiceras på Ineras webbplats.

Om något förhållande som påverkar en direktansluten producents HPT förändras **ska** ny policytillämpning inlämnas skyndsamt. Den nya versionen **ska** baseras på aktuell mallversion.

2.3 Förpliktelser för konsumerande organisation

2.3.1 Allmänt

Konsument **ska** arbeta enligt denna policy och garantera att samtliga krav avseende konsumenter efterlevs.

Om informationen lagras i konsumentens egen applikation **får ej** informationen från HSA ändras. Konsumenten ansvarar för att informationen hålls uppdaterad och aktuell.

2.3.2 Förpliktelser för kontaktperson hos konsumerande organisation

Kontaktperson för konsument som använder information från HSA **ska** tillse att:

- informationshanteringen sker i enlighet med HSA-policyn och godkänd HPT Konsument
- behandling av personuppgifter följer EU:s dataskyddsförordning (GDPR)
- - om personuppgifter från HSA hanteras i tjänsten - regelbunden teknisk uppföljning av aktuell säkerhetsnivå, t.ex. automatiserad sårbarhetsskanning, intern granskning av säkerhetsfunktioner och/eller intrångstester med hjälp av tredje part, sker
- kontinuitetsplanering (avbrotts- och katastrofplanering) finns i händelse av att HSA ej är tillgänglig
- ett dokumenterat regelverk finns för hur användare ges tillgång till information som härstammar från HSA och för hur behörigheter tilldelas

- eventuella begränsningar i belastning på HSA efterlevs
- Riktlinjer för tester och testdata i HSA [6] efterlevs
- personer som arbetar med HSA-information inom tjänsten har kännedom om och arbetar i enlighet med HSA-policyn och HPT
- HSA-information raderas ur tjänsten när avtal om HSA-anslutning upphör.
    - Undantag från denna regel kan beviljas av HSA Policygrupp, till exempel utifrån legala krav på spårbarhet.

Kontaktpersonen ansvarar för löpande kontakter med HSA Förvaltning och andra intressenter inom HSA.

2.3.3 HSA-policytillämpning för konsument (HPT Konsument)

Konsumenten **ska** ta fram ett särskilt dokument, ”HSA-policytillämpning för konsument” (HPT Konsument), som beskriver hur denna policy tillämpas. Framtagen HPT **ska** godkännas av HSA Policygrupp.

HPT **ska** utformas enligt anvisningarna i dokumentet ”Mall för HSA-policytillämpning för konsument” [4].

HPT Konsument **ska** innehålla en redogörelse för vilken information som används och hur denna nyttjas.

Godkänd HPT **ska** arkiveras av konsumenten. Namn på tjänst och organisation som har godkänd HPT kommer att publiceras på Ineras webbplats.

Om något förhållande som påverkar en konsuments HPT förändras **ska** ny policytillämpning inlämnas skyndsamt. Den nya versionen ska baseras på aktuell mallversion.

2.4 Särskilda förpliktelser för HSA-ombud

HSA-ombud **ska** ansvara för sina tredjepartsanslutna organisationer, som om de gällde deras egen organisation, för allt som sägs i denna policy. Det inkluderar även genomförande av internrevision.

HSA-ombud **ska** tillse att tredjepartsanslutning endast sker av organisationer inom vård- och omsorgssektorn. Samarbetsavtal som omfattar hanteringen i HSA, inklusive reglering av informationsägarskap och informationssäkerhetsansvar, **ska** finnas mellan HSA-ombud och tredjepartsanslutna organisationer. Samarbetsavtalen **ska** på uppmaning delges HSA Förvaltning.

HPT Producent **ska** innehålla en lista på de tredjepartsanslutna organisationerna som finns på o-nivå. För tredjepartsanslutna organisationer på ou-nivå **ska** beskrivas hur dessa kan urskiljas från organisationens/organisationernas (o) egna objekt.

HPT Konsument **ska** innehålla en beskrivning av vilka tredjepartsanslutna organisationer/tjänster som nyttjar HSA-information via organisationen.

HSA-ombud **ska** ha en organiserad supportfunktion för tredjepartsanslutna organisationers HSA-relaterade ärenden.

2.5 Informationsinnehåll i HSA

Informationsinnehållet i HSA **ska** följa den specifikation som anges i aktuell ”Informationsspecifikation för Katalogtjänst HSA” [2] med tillhörande bilagor som specificerar innehåll i HSA. Gällande HSA-schema finns publicerat på Ineras webbplats.

Vid uppgradering av HSA-schemat **bör** ansluten producent utan dröjsmål anpassa lokal katalog eller motsvarande så att gällande schema följs. Förändringar **ska** vara införda senast tre månader efter uppgradering av HSA-schemat.

2.6 Hantering av andra organisationers information

Ansluten producent **får ej** tillgängliggöra HSA-information från andra anslutna producenter utanför den egna organisationen, t.ex. genom publicering på Internet eller annan spridning av information till tredje part, såvida inte särskild överenskommelse finns med den organisation vars uppgifter publiceras.

Anslutna producenter och konsumenter **får ej** tillgängliggöra HSA-information på annat sätt än vad som beskrivs i godkänd HPT.

Information från HSA **får ej** användas för massutskick i marknadsföringssyfte. Konsument **får ej** ta betalt för HSA-information.

2.7 Revision

Direktansluten producerande och konsumerande organisation **ska** löpande, med max 13 månaders mellanrum, genomföra internrevision för att kontrollera efterlevnad av krav i denna policy. Internrevision kan till exempel omfatta genomgång av samtliga rutiner kopplade till HSA-hanteringen, stickprovskontroller av innehåll och/eller enkäter till eller besök hos lokala administratörer för att säkerställa att organisationens rutiner följs. Vid revision **ska** dessutom policytillämpningens aktualitet och överensstämmelse med policyn kontrolleras. Genomförda revisioner **ska** dokumenteras och dateras.

HSA-ombud **ska** genomföra internrevision som omfattar tredjepartanslutna organisationer. Internrevision **bör** omfatta samtliga tredjepartanslutna organisationer varje år och samtliga tredjepartsanslutna organisationer **ska** ha omfattats av internrevision minst vart tredje år.

Revisionsrapporter **ska** vid förfrågan delges HSA Förvaltning. Allvarliga brister som påträffas lokalt som riskerar att påverka andra anslutna producenter eller konsumenter **ska** omedelbart rapporteras till HSA Förvaltning.

HSA Förvaltning, eller av HSA Förvaltning utsedd tredje part, **får** genomföra revision av ansluten producent eller konsument för att kontrollera efterlevnad av denna policy.

Eventuella brister och avvikelser som påträffas vid en revision **ska** åtgärdas skyndsamt, allvarliga brister **ska** åtgärdas inom 6 månader.

Om HSA Policygrupp bedömer det nödvändigt att genomföra förnyad revision bekostas denna av ansluten producent eller konsument.

3 Styrning av HSA

3.1 Övergripande styrning och ansvarsförhållanden

Systemägare för HSA är VD för Inera AB.

Systemägaren ansvarar för att utse lämpliga stödfunktioner för central förvaltning av HSA, inklusive förvaltningsansvarig. Policygruppen och dess ordförande utses av Ineras programråd.

Policygruppen svarar för att, i samråd med av systemägare utsedd förvaltningsansvarig och inom ramen för godkänd förvaltningsplan, främja utveckling och användning av HSA genom förslag angående t.ex. förändringar och tillägg i policy, schema och regelverk, nya anslutningar etc.

Löpande förvaltningsfrågor handläggs av förvaltningsansvarig som, efter delegering från systemägare och i samråd med policygruppen, kan fatta beslut i HSA-frågor.

3.2 Godkännandeprocess vid anslutning till HSA

Godkännandeprocessen för anslutande producenter och konsumenter innehåller följande steg:

1. Anslutande producent eller konsument ansöker om anslutning.
2. Efter utredning av anslutning tar anslutande producent fram HPT Producent och konsument tar fram HPT Konsument.
3. Granskning sker av HPT.
4. Resultatet av granskningen redovisas i HSA Policygrupp som tar ställning till godkännande.
5. När HPT är godkänd undertecknas anslutningsavtal.

Förändringar i HPT **ska** godkännas av HSA Policygrupp.

4 Informationssäkerhetskrav

4.1 Allmänt

För att bibehålla tilliten mellan de producerande och konsumerande organisationer som använder HSA är det viktigt att det interna informationssäkerhetsarbetet sker på ett strukturerat sätt så att en likvärdig nivå kan upprätthållas mellan organisationerna. Informationssäkerhetsarbetet ska utgå från de fyra aspekterna riktighet, tillgänglighet, konfidentialitet och spårbarhet. Detaljerad vägledning kring kraven i detta kapitel ges bland annat av Myndigheten för samhällsskydd och beredskaps föreskrifter och allmänna råd om statliga myndigheters informationssäkerhet [9] samt i den internationella standarden ISO/IEC 27002 [10].

Såväl ansluten producent som ansluten konsument **bör** ha ett ledningssystem för informationssäkerhet (LIS) eller en informationssäkerhetspolicy och arbeta i enlighet med denna. Detta krav finns redan på vårdgivare i enlighet med Socialstyrelsens föreskrifter HSLF-FS 2016:40.

4.2 Krav på riktighet

Strukturen i HSA kan se olika ut beroende på olika organisationers indelning i ekonomiska, organisatoriska och ansvarsmässiga enheter. Rekommendationen är att organisationens struktur i HSA utgår från enheter med egen budget, egen personal och en formellt ansvarig chef.

Informationsinnehållet i HSA **ska** vara korrekt och aktuellt, det vill säga spegla nuläget i organisationen när det gäller medarbetare, organisation och funktioner.

Informationsinnehållet i HSA **ska** när så är möjligt hämtas elektroniskt från annan kvalitetssäkrad grunddatakälla, t.ex. från folkbokföringsregister och Socialstyrelsens register över legitimerad hälso- och sjukvårdspersonal (HOSP).

Informationsinnehållet i HSA **ska** när så är möjligt kontrolleras och vid behov uppdateras regelbundet, minst en gång i månaden, via automatiska kontroller.

Information i beskrivningar och fritextfält **får inte** vara stötande eller kränkande. Den **ska** vara informativ och relevant utan värderingar och jämförelse med andra.

Ansluten producents lokala rutiner för uppdatering av information i HSA **ska** vara dokumenterade samt kända och implementerade i organisationen. Lokala rutiner **ska** på begäran delges HSA Förvaltning.

Ansluten konsument **ska** tillse att HSA-information raderas ur tjänsten när avtal om HSA-anslutning upphör. Undantag från denna regel kan beviljas av HSA Policygrupp, till exempel utifrån legala krav på spårbarhet.

4.2.1 Personuppgifter

Personuppgifter **ska** vid registrering samt regelbundet, minst en gång i månaden, verifieras mot Skatteverkets register med hjälp av personnummer eller samordningsnummer. HPT Producent **ska** innehålla en beskrivning av hur personuppgifter verifieras.

Uppgifter om legitimation, specialistkompetens och förskrivningsrätt **ska** hämtas från Socialstyrelsens register över legitimerad hälso- och sjukvårdspersonal (HOSP) samt regelbundet, minst en gång i månaden, verifieras mot samma källa.

Personer i HSA **ska** ha ett anställnings- eller uppdragsförhållande till den organisation de tillhör i HSA. Verifiering av att anställnings- eller uppdragsförhållandet kvarstår **ska** göras vid registrering samt minst en gång per kvartal. Undantag kan göras för studenter, vars uppdragsförhållande får kontrolleras terminsvis, förutsatt att detta beskrivs i godkänd HPT Producent.

I det fall svenskt personnummer eller samordningsnummer saknas **ska** verifiering av personuppgifter ske med hjälp av uppvisad identitetshandling (enligt definition i Informationsspecifikation Katalogtjänst HSA [2]). En kopia av identitetshandlingen **ska** arkiveras hos organisationen. Identitetshandlingens nummer och giltighetstid **ska** registreras i HSA tillsammans med personens födelsedatum. Personobjektet i HSA **får ej** ha längre giltighetstid än identitetshandlingen.

4.2.2 Organisationsuppgifter

Vid skapandet av organisationsuppgifter **ska** dessa verifieras mot SCB:s och/eller Bolagsverkets register genom användning av organisationsnummer. HPT Producent **ska** innehålla en beskrivning av hur organisationsuppgifter verifieras.

Vid avslut av organisationer på organisationsnivå (o-nivå) i HSA **ska** organisationen arkiveras i HSA med namn, HSA-id, organisationsnummer och namn på godkänd HPT.

4.2.3 Vårdgivare och vårdenheter

Organisationer som anges som Vårdgivare i HSA **ska** finnas registrerade i Inspektionen för vård och omsorgs (IVO) Vårdgivarregister, det vill säga vårdgivarens organisationsnummer ska återfinnas vid sökning i Vårdgivarregistret.

Vårdenheter och verksamhetschefer som anges i HSA **ska** vara korrekta och uppdaterade enligt vårdgivarens beslut.

Vårdgivare och vårdenheter **får ej** tas bort från HSA när de upphör med sin verksamhet. Istället **ska** de arkiveras i HSA. Om en vårdenhet byter vårdgivare **ska** vårdenheten arkiveras och en ny vårdenhet skapas.

För vårdgivare **ska** namn, HSA-id, organisationsnummer samt eventuellt start- och slutdatum sparas. För vårdenheter **ska** namn, HSA-id, eventuellt start- och slutdatum samt vårdgivartillhörighet sparas.

4.2.4 HSA-id

Alla objekt i HSA **ska** identifieras med HSA-id. HSA-id **ska** vara unikt och uppbyggt enligt gällande syntax.

Kopplingen mellan HSA-id och person-id **ska** arkiveras om informationen tas bort från HSA. Varje ansluten producerande organisation **ska** själv besluta om arkiveringstid med hänsyn till gällande lagstiftning (såväl GDPR:s principer för lagringsminimering som lagstiftning kopplad

till krav på spårbarhet för t.ex. åtkomst till patientdata). Periodicitet, arkiveringstid och procedurer för arkivering beskrivs i HPT Producent.

Vid byte av person-id (t.ex. från samordningsnummer till personnummer) **får ej** HSA-id ändras. Undantag **ska** göras i känsliga fall som t.ex. byte av person-id på grund av hot och våld där koppling mellan tidigare och nytt person-id saknas i folkbokföringsregistret. Tidigare person-id **bör inte** lagras, inte ens i Limbo eller motsvarande struktur för inaktiva personer.

4.2.5 Särskilt tillstånd kring fingerade data i monitorerings- och verifieringssyfte

Fingerade data i HSA:s produktionsmiljö **får ej** förekomma utan särskilt tillstånd.

Under vissa förutsättningar kan en producent eller konsument undantagsvis få tillåtelse att registrera och använda fingerade data i en utpekad gren i HSA i verifierings- eller monitoreringssyfte. Detta **ska** föregås av ett godkännande i HSA Policygrupp. Begäran om ett sådant undantag **ska** vara skriftlig och beskrivas i producentens eller konsumentens HPT.

Hanteringen av fingerade data **ska** följa riktlinjerna för tester och testdata i HSA [6].

4.3 Krav på tillgänglighet

Målsättningen är att HSA är tillgängligt dygnet runt under årets alla dagar. Detta ska vara utgångspunkten för såväl drift som applikationsutveckling av HSA.

Om HSA uppdateras från lokal katalog eller motsvarande **bör** samma målsättning gälla för den lokala tjänsten.

Om LDAP används vid kommunikation med HSA **ska** HSA LDAP-policy [7] följas.

4.4 Krav på spårbarhet

Förändringar i HSA **ska** loggas.

Loggning **ska** ske på ett sådant sätt att all förändring av informationsinnehåll i HSA kan spåras. Loggfiler **ska** innehålla information om vilken förändring som gjorts, om användaren/systemet som gjorde förändringen och tidpunkten för förändringen.

Loggningen **ska** ske på ett sådant sätt att ansvarig administratör kan identifieras.

Loggfiler innehållande förändringar av HSA-information som lagras nationellt **ska** lagras i fem år enligt beslut från Inera AB. Beslutet är fattat mot bakgrund av att preskriptionstiden för dataintrång (som kan bli följden av en felaktig registrering av behörighetsgrundande information i HSA) är fem år.

Om HSA uppdateras från lokal katalog eller motsvarande ställs samma krav på den lokala tjänsten, inklusive att fastställa hur länge loggar ska sparas med hänsyn till gällande lagstiftning. För mer vägledning kring loggning se [9] och [10].

4.5 Krav på sekretess

Information som kräver utökad behörighet **ska** endast kunna registreras av och visas för behöriga administratörer. Åtkomst till HSA-information **ska** regleras i enlighet med HSA Informationsklassning [11].

Skyddade personuppgifter **ska** vara dolda i HSA och endast hanteras av ett fåtal utsedda administratörer. Personer med skyddade personuppgifter **ska** informeras av arbetsgivaren om hur personuppgifterna hanteras och **bör** kunna välja om uppgifterna ska göras synliga.

Ansluten producents rutiner för hantering av skyddade personuppgifter **ska** beskrivas i HPT. Av beskrivningen **ska** det framgå hur personuppgifter döljs i samband med att en person får skyddade personuppgifter samt hur uppgifterna synliggörs när personen inte längre har skyddade personuppgifter.

Konsumenter får endast tillgång till skyddade personuppgifter i undantagsfall och efter en riskbedömning. De konsumenter som får tillgång till dessa uppgifter **ska** i HPT beskriva hur uppgifterna hanteras.

All kommunikation mot HSA **ska** vara krypterad.

Om HSA uppdateras från lokal katalog eller motsvarande ställs samma krav på den lokala tjänsten. Kommunikation med interna källsystem över organisationsinterna nätverk **får** ske okrypterat, förutsatt att säkerheten ändå anses kunna garanteras och att detta undantag beskrivs i godkänd HPT Producent, fullständig.

4.6 Kontinuitetsplanering

Ansluten producent och konsument ansvarar för egen kontinuitetsplanering i händelse av störningar i HSA. Organisationens kontinuitetsplan för HSA **bör** dokumenteras av producent och konsument.

4.7 Säkerhetskopiering

Säkerhetskopiering av information i HSA **ska** ske regelbundet, minst en gång per dygn om förändring av informationsinnehåll gjorts.

Säkerhetskopior **ska** förvaras avskilt från HSA.

Om HSA uppdateras från lokal katalog eller motsvarande ställs samma krav på den lokala tjänsten. För mer vägledning kring säkerhetskopiering se [9] och [10].

4.8 Skydd mot intrång

HSA **ska** skyddas säkerhetsmässigt mot otillbörlig åtkomst samt mot otillbörlig förändring av informationen. Tillträde – såväl fysiskt som via systemadministration och fjärråtkomst från annan plats – till servrar e.d. innehållande HSA-information **ska** vara begränsat till personal med särskild behörighet. Detaljerad beskrivning av behörighetsregler och procedurer för tillträde **ska** dokumenteras.

Om personuppgifter från HSA hanteras i tjänsten **ska** regelbunden teknisk uppföljning ske av aktuell säkerhetsnivå. Sådan uppföljning kan innefatta automatiserad sårbarhetsskanning, intern granskning av säkerhetsfunktioner och/eller intrångstester med hjälp av tredje part.

Om HSA uppdateras från lokal katalog eller motsvarande ställs samma krav på den lokala tjänsten. För mer vägledning kring fysisk säkerhet och administrationssäkerhet, se [9] och [10].

4.9 Styrning av åtkomst

Åtkomst av information i HSA **ska** föregås av autentisering direkt av individ eller indirekt via annat system. Behörighet till olika informationsmängder **ska** regleras i enlighet med HSA Informationsklassning [11].

Om konsument använder behörighetsgrundande information från HSA **ska** behörighetsmodellen beskrivas i HPT Konsument.

För mer vägledning kring styrning av åtkomst, se [9] och [10].

4.9.1 Styrning av åtkomst för HSA-administratörer

Detaljerad beskrivning av procedurer för behörighetshantering för administratörer **ska** dokumenteras och redovisas i HPT Producent.

Administratörer **ska** identifiera sig med stark autentisering. Metod för stark autentisering **bör** vara SITHS-certifikat. Om annan metod används **ska** denna beskrivas i HPT Producent.

Om HSA uppdateras från lokal katalog eller motsvarande ställs samma krav på den lokala tjänsten.

4.9.2 Styrning av åtkomst för konsument

Konsumenten ansvarar för att följa HSA:s riktlinjer för åtkomst vid användning av HSA-information. Tilldelad behörighet **får ej** delas vidare till annan part.

Refererade dokument

[1]	HSA-policy
[2]	Informationsspecifikation för Katalogtjänst HSA
[3]	Mall för HSA-policytillämpning för producent, HPT-mall Producent
[4]	Mall för HSA-policytillämpning för konsument, HPT-mall Konsument
[5]	Mall för anslutningsavtal
[6]	Riktlinjer för tester och testdata i HSA
[7]	HSA LDAP-policy
[8]	HSA Begrepp och definitioner
[9]	Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2016:1) samt www.informationssakerhet.se
[10]	SS-EN ISO/IEC 27002:2017, Informationsteknik - Säkerhetstekniker - Riktlinjer för informationssäkerhetsåtgärder
[11]	HSA Informationsklassning

Förkortningar

HOSP	Socialstyrelsens register över legitimerad hälso- och sjukvårdspersonal
HPT	HSA-policytillämpning, finns för producent och för konsument
LDAP	Lightweight Directory Access Protocol
GDPR	Europaparlamentets och rådets förordning (EU) nr 2016/679. GDPR är förkortning för General Data Protection Regulation.

Begrepp och definitioner finns beskrivna i särskilt dokument [8].