HSA-policytillämpning för producent

Region Skåne

Version 6.0 2019-06-17

Instruktioner för ifyllnad av HPT finns på sidan 4 i detta dokument. Läs instruktionerna innan du börjar arbeta med dokumentet.

Innehåll

Kontaktuppgifter

Denna HSA-policytillämpning förvaltas av:

Organisation: Skåne Läns Landsting
Adress: Region Skåne
Postnummer: 29189
Ort: Kristianstad
Telefon: 044-309 30 00
E-post: region@skane.se
Webbplats: www.skane.se

Instruktion för ifyllnad av HPT – Läs mig först!

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. Varje ansluten organisation tar fram och förvaltar en HSA-policytillämpning (HPT) som beskriver att – och hur – organisationen uppfyller HSA-policyn.

Denna mall är framtagen för att anslutna organisationer ska beskriva sin hantering av HSA-information på ett likartat sätt. Mallen följer avsnittsindelningen i HSA-policyn för att det ska vara lätt att känna igen sig. Det finns sammanlagt fyra olika mallar för HSA-policytillämpning:

1. *HPT Producent HSA Admin (förenklad)*
2. *HPT Producent (fullständig)*
3. *HPT Konsument Publik enhetsinformation (förenklad)*
4. *HPT Konsument (fullständig)*

För varje krav som är relevant för anslutningsformen finns en beskrivning av kravet och antingen en kryssruta för att bekräfta att du läst och förstått kravet eller en fritextruta där du beskriver organisationens rutiner som används för att säkerställa att kravet uppfylls. Det finns också rutor med plats för t.ex. namn, roller och kontaktuppgifter.

Det är endast de grå kryss- och fritextrutorna i dokumentet som går att fylla i. Genom att använda tangentbordets tab-tangent kan du växla mellan ifyllningsbara fält. Bara Tab växlar till nästa fält. Shift+Tab växlar till föregående fält.

Innan ett fält har fyllts i står en instruktionstext i fältet. Denna ska tas bort helt, även klamrarna runt om instruktionen.

Till varje ifyllningsbart fält finns en hjälptext som beskriver vad som ska stå i fältet. Du får fram denna genom att trycka på knappen F1 på ditt tangentbord (fungerar ej för Mac) när markören står i det aktuella fältet. Den första delen av hjälptexten står också längst ner i fönstret, till vänster i den grå/blå ramen (fungerar även för Mac). Använd alltid hjälpfunktionen (F1) för att säkerställa att du fyllt i fältet med rätt information.

Alla kryssrutor och fritextfält i HPT ska fyllas i, utom när det tydligt framgår att du ska välja ett av alternativen. Kryssrutor kan klickas i eller fyllas genom att använda X-tangenten.

Spara din HPT med dokumentnamnet [typ_av_HPT]_[Organisationens_namn]_[version].docx, t.ex. HPT_Producent_HSA_Admin_Inera_AB_2.1.docx.

När HPT är fullständigt ifylld ska den skickas till Ineras Kundservice. Verifiera en sista gång att alla fält är ifyllda (även på dokumentets förstasida och under rubriken Kontaktuppgifter på sidan 3) samt att versionsnummer och datum är korrekt, både i revisionshistoriken och på dokumentets förstasida.

Revisionshistorik

Versioner numreras enligt följande:

- *Den allra första versionen, innan en organisation blivit godkänd för första gången, numreras 0.1*
- *Vid eventuell komplettering av den ansökande organisationen ökas numreringen på andra siffran till 0.2, 0.3 o.s.v.*
- *När HPT godkänns av HSA Policygrupp för första gången sätts versionen till 1.0*
- *När den anslutande organisationen uppdaterar HPT ökas numreringen på andra siffran till 1.1, 1.2 o.s.v.*
- *När HPT godkänns av HSA Policygrupp för andra gången sätts versionen till 2.0*
- *Nästa uppdatering från anslutande organisation blir då 2.1, nästa godkända version får 3.0 o.s.v.*

OBS! Revisionshistorik från tidigare HPTA / HPT Producent ska också finnas i tabellen.

OBS! Mallversionsnumret (4.1 i detta dokument) har inget att göra med versionsnumreringen av HPT i tabellen nedan.

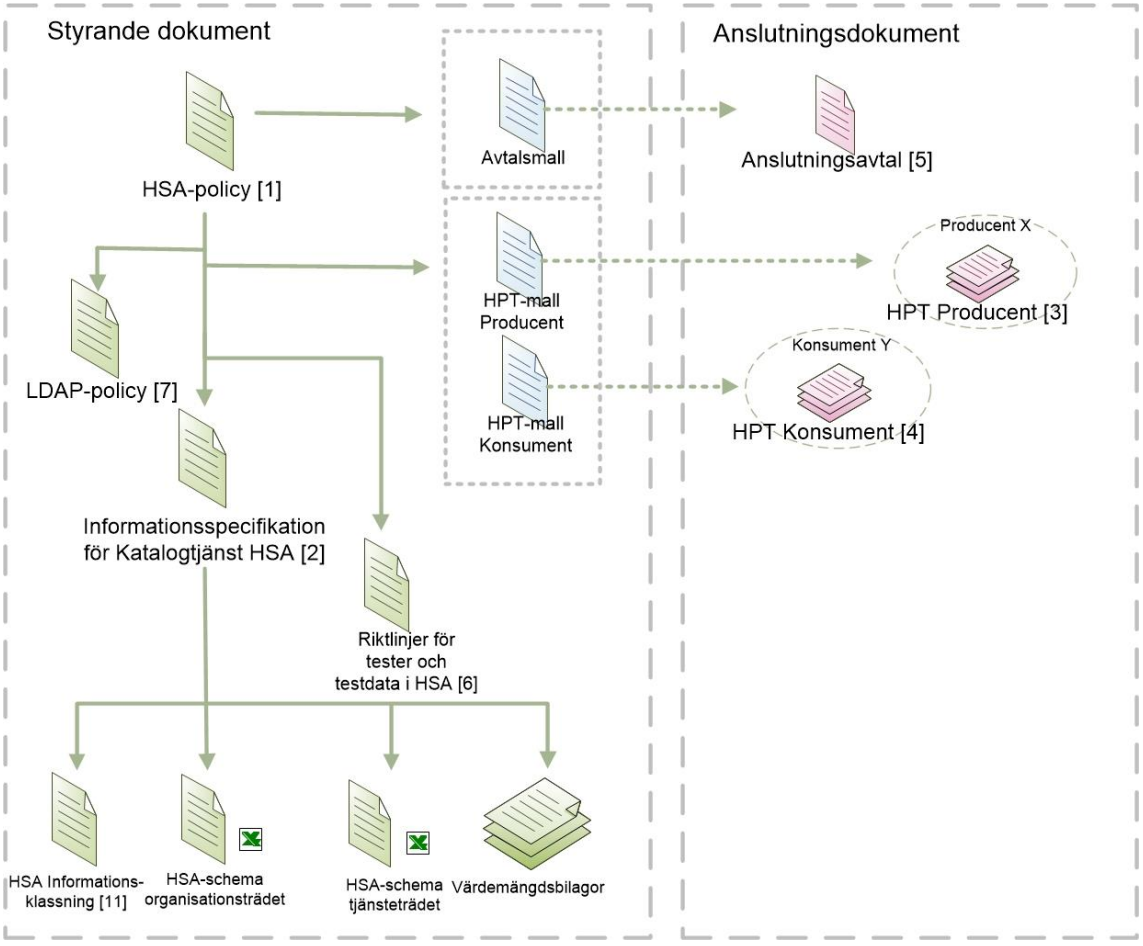
Om raderna för versioner tar slut, kontakta HSA Förvaltning för hjälp.

Version	Datum	Kommentar
1.0	2013-01-14	Anmärkningar åtgärdade
2.0	2013-02-05	Godkänd av Inera
2.1	2013-05-23	Anpassad till mall 3.6
2.2	2013-12-12	Anmärkningar åtgärdade
2.3	2014-03-05	Anpassad till regional HSA-nod stängts samt anmärkningar åtgärdade
3.0	2014-03-14	Godkänd av HSA Förvaltningsgrupp
3.1	2015-03-05	Byte av kontaktuppgifter. Rev kap 4.2.1 samt rättning av stavfel
4.0	2015-03-11	Godkänd av HSA Förvaltningsgrupp
4.1	2017-02-24	Omarbetad pga ny mall
4.2	2017-04-27	Diverse justeringar. Anmärkningar åtgärdade enligt granskningsrapport 17-03-17
4.3	2017-06-08	Anmärkningar åtgärdade enligt granskningsrapport 17-05-09 Kap 4.2, ruta nr 3. Kap 4.2.1, huvudadministratör korrigerar uppgifterna. Förtydligande om verifiering Kap 4.2.5 förtydligande

Version	Datum	Kommentar
5.0	2017-06-15	Godkänd av HSA Förvaltningsgrupp
5.1	2019-02-25	Omarbetad pga ny HSA-ansvarig
5.2	2019-04-18	Anmärkningar åtgärdade enligt granskningsrapport 19-02-28 bortsett från de ang. 4.2.4 p.g.a. utlåtande från regionjurist. Ändring i 4.2.1 ang. kontroll av skyddade personer Lagt till 3 anrop i bilaga 2
5.3	2019-05-03	Anmärkningar åtgärdade enligt granskningsrapport 19-05-03 bortsett från punkt 7 Revisionshistorik justerades - fel datum för version 5.x
5.4	2019-05-03	Ändring i bilaga 2: "Mina tjänster" blir "Mina Planer"
5.5	2019-05-28	Ändringar i bilaga 2 enligt granskningsrapport 19-05-28
6.0	2019-06-17	Godkänd av HSA Policygrupp

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]**, 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

Denna variant av HSA-policytillämpning är avsedd för producerande organisationer som har en fullständig anslutning till HSA.

☒ Vår organisation bekräftar efterlevnad av HSA-policyn genom anslutningsavtal och upprättande av denna policytillämpning (HPT Producent) och förbinder sig att efterleva HSA-policyn enligt denna tillämpningsbeskrivning.

1.2 Begrepp och definitioner

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

1.3 Syfte med HSA och HSA-policyn

Syftet med HSA och HSA-policyn beskrivs i HSA-policyn [1].

1.4 Målgrupp och tillämplighet

Målgrupper för denna HSA-policytillämpning, utöver HSA Policygrupp, är HSA-ansvarig samt beslutsfattare hos den anslutna producerande organisationen.

2 Allmänna förutsättningar

2.1 Ansvarsförhållanden

☒ Vår organisation har en utsedd huvudansvarig för anslutningen till HSA, kallad HSA-ansvarig. HSA-ansvarig för vår organisation är Jonatan Åstrand-Ferris, Handläggare/IT och sammankallande verksamhetsansvarig för koncernkontoret i förvaltningsgruppen för den lokala HSA- och verksamhetskatalogen.

☒ HSA-ansvarig i vår organisation har tillräckliga mandat och kontaktvägar inom organisationen för att kunna hantera alla kontakter rörande HSA-frågor.

☒ Vår organisation har utsett en ställföreträdande HSA-ansvarig som kan täcka upp för HSA-ansvarig under kortare frånvaro (t.ex. semester). Vi är medvetna om att vår organisation bör anmäla denna person till HSA Förvaltning för att ges samma rättigheter som HSA-ansvarig.

2.2 Förpliktelser för producerande organisation

2.2.1 Allmänt

☒ Vår organisation arbetar enligt HSA-policyn och garanterar att organisationen efterlever samtliga policykrav.

2.2.2 Förpliktelser för HSA-ansvarig hos direktansluten producerande organisation

☒ HSA-ansvarig i vår organisation har genomgått en av Inera AB godkänd grundutbildning för HSA

☒ HSA-ansvarig i vår organisation tar ansvar för 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 samt till eventuella tredjepartsanslutna 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.

☒ Eftersom vår organisation har en fullständig anslutning till HSA tar HSA-ansvarig i vår organisation även ansvar för:

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

2.2.3 HSA-policytillämpning för producent (HPT Producent)

☒ Vår organisations HPT är utformad enligt anvisningarna i dokumentet HPT-mall Producent [3] och beskriver all vår användning av HSA.

Följande system/verksamheter/tjänster inom vår organisation använder HSA (anrop mot HSA kataloghotell):

Microsoft Identity Manager(MIM) synkroniserar data till HSA. Finns en tjänst för att hämta data från Hosp i HSA (se bilaga nedan).

Lokal säkerhetstjänst använder HsaWs vid inloggning.

Lokalt tjänstekontraktsanrop (getEmployeeIncludingProtectedPerson) nyttjas av den lokala tjänsten Mina planer, som används för sammanhållen vårdplanering för region och kommuner.

Användningen beskrivs mer utförligt i Bilaga 2.

☒ Vår organisation arkiverar godkänd HPT och godkänner att uppgifter om vår godkända HPT publiceras på Ineras webbplats.

☒ Om något förhållande som påverkar vår organisations HPT ändras lämnar vi in en ny policytillämpning som är baserad på aktuell mallversion.

2.3 Förpliktelser för konsumerande organisation

Ej tillämplig för HPT Producent.

2.4 Särskilda förpliktelser för HSA-ombud

Välj ett av de två nedanstående alternativen.

☐ Vår organisation agerar inte HSA-ombud, d.v.s. registrerar inte information om någon annan organisation eller verksamhet som inte är vår egen.

☒ Vår organisation agerar HSA-ombud, och vi förbinder oss därför

- att ansvara för våra tredjepartsanslutna organisationer, som om de gällde vår egen organisation, för allt som sägs i denna policy, vilket även inkluderar genomförande av internrevision
- att tredjepartsanslutning endast sker av organisationer inom vård- och omsorgssektorn
- att samarbetsavtal som omfattar hanteringen i HSA, inklusive reglering av informationsägarskap och informationssäkerhetsansvar, finns mellan vår organisation och våra tredjepartsanslutna organisationer
- att på uppmaning delge HSA Förvaltning våra samarbetsavtal
- att tillhandahålla en organiserad supportfunktion för tredjepartsanslutna organisationers HSA-relaterade ärenden

Följande tredjepartsanslutna organisationer är upplagda på organisationsnivå (o-nivå) i HSA: <saknas>.

Tredjepartsanslutna organisationer som finns på enhetsnivå (ou-nivå) i HSA kan urskiljas från vår organisations egna objekt i HSA på följande vis: Attributet organisationsnummer, orgNo, anger vilken organisation katalogobjektet enhet tillhör. Till yttermera visso är externa organisationer (med ett fåtal undantag) placerade i separata kataloggrenar.

2.5 Informationsinnehåll i HSA

☒ Vår organisations informationsinnehåll i HSA följer den specifikation som anges i aktuell ” Informationsspecifikation för Katalogtjänst HSA” [2] med tillhörande bilagor som specificerar innehåll i HSA. Vi är medvetna om att gällande HSA-schema finns publicerat på Ineras webbplats.

☒ Vår organisations lokala katalog eller motsvarande anpassas utan dröjsmål, senast tre månader efter uppgradering av HSA-schemat, så att gällande schema följs.

2.6 Hantering av andra organisationers information

☒ Vår organisation tillgängliggör inte 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 organisationen/organisationerna vars uppgifter publiceras.

Publicering på 1177.se sker enligt specifikation i avtal mellan Region Skåne och tredje part.

☒ Vår organisation tillgängliggör inte HSA-information på annat sätt än vad som beskrivs i godkänd HPT.

☒ Vår organisation använder inte information från HSA för massutskick i marknadsföringssyfte**.**

☒ Vår organisation tar inte betalt för annan organisations HSA-information**.**

2.7 Revision

☒ Vår organisation genomför löpande, med max 13 månaders mellanrum, internrevision för att kontrollera efterlevnad av krav i HSA-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 kontrollerar vår organisation dessutom policytillämpningens aktualitet och överensstämmelse med policyn.

☒ Vår organisations genomförda revisioner dokumenteras och dateras.

☒ Vår organisation delger HSA Förvaltning våra revisionsrapporter vid förfrågan.

☒ Vår organisation rapporterar omedelbart eventuella allvarliga brister som upptäcks vid revision till HSA Förvaltning.

☒ Vår organisation accepterar att HSA Förvaltning, eller av HSA Förvaltning utsedd tredje part, får genomföra revision för att kontrollera vår organisations efterlevnad av HSA-policy.

☒ Vår organisation åtgärdar eventuella brister och avvikelser som påträffas vid en revision skyndsamt, allvarliga brister åtgärdas alltid inom 6 månader.

☒ Om HSA Policygrupp bedömer det nödvändigt att genomföra förnyad revision bekostas denna av vår organisation.

Välj ett av de två nedanstående alternativen.

☐ Vår organisation agerar inte HSA-ombud, d.v.s. registrerar inte information om någon annan organisation eller verksamhet som inte är vår egen.

☒ Vår organisation agerar HSA-ombud, och vi förbinder oss därför

- att genomföra internrevision som omfattar tredjepartanslutna organisationer
- att tillse att alla tredjepartsanslutna organisationer ska ha omfattats av internrevision minst vart tredje år

3 Styrning av HSA

3.1 Övergripande styrning och ansvarsförhållanden

Styrning av HSA på övergripande nivå sker enligt kapitel 3 i HSA-policyn [1].

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.

Vid eventuella förändringar i godkänd HPT inlämnas en ny version för godkännande i HSA Policygrupp.

4 Informationssäkerhetskrav

4.1 Allmänt

Vägledning kring informationssäkerhetskraven framgår av HSA-policy [1].

☒ Vi är medvetna om att vår organisation 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

☒ Vår organisations informationsinnehåll i HSA är korrekt och aktuellt, det vill säga speglar nuläget i organisationen när det gäller medarbetare, organisation och funktioner.

☒ Vår organisation kontrollerar och uppdaterar vid behov informationsinnehållet i HSA via automatiska kontroller. Detta gör vi genom att huvudadministratör kontrollerar och vid behov uppdaterar HSA-informationen utifrån t.ex. följsamhet till värdemängder och personer med passerat slutdatum. För detta ändamål använder vi HSA portalen för kvalitetskontroll. Kontrollen/kontrollerna genomförs första tisdagen varje månad.

☒ Vår organisation säkerställer att information i beskrivningar och fritextfält inte är stötande eller kränkande, att den är informativ och relevant utan värderingar och jämförelse med andra.

☒ Vår organisations lokala rutiner för uppdatering av information i HSA är dokumenterade samt kända och implementerade i organisationen.

☒ Vår organisation delger HSA Förvaltning de lokala rutinerna på begäran.

4.2.1 Personuppgifter

Inera AB ansöker regelbundet om utdrag av information om legitimation, specialistkompetens och förskrivningsrätt för personer registrerade i HSA hos Socialstyrelsen, vilken sedan kan användas av HSA-ansluten organisation för att uppdatera uppgifter.

Välj ett av de två nedanstående alternativen.

☒ Vår organisation tillåter att Inera AB ansöker om detta utdrag även för vår organisations räkning.

☐ Vår organisation tillåter inte att Inera AB ansöker om detta utdrag även för vår organisations räkning. Vi är medvetna om att det innebär att vi inte kan använda t.ex. HSA-portalen för kontroll av dessa uppgifter utan istället behöver verifiera dessa manuellt hos Socialstyrelsen och att samma krav på månatliga kontroller av all information gäller för oss.

På följande sätt verifierar vår organisation personuppgifter i HSA.

☒ Vår organisations uppgifter om legitimation, specialistkompetens och förskrivningsrätt hämtas från Socialstyrelsens register över legitimerad hälso- och sjukvårdspersonal (HOSP) och verifieras regelbundet, minst en gång i månaden, mot samma källa. Detta säkerställer vi genom att i samband med förändringar hämtas information löpande från HOSP i HSA via LDAP. Kontrollen genomförs en gång per dygn.

☒ Vår organisations personuppgifter verifieras vid registrering samt regelbundet, minst en gång i månaden, mot Skatteverkets register med hjälp av personnummer eller samordningsnummer. Detta säkerställer vi genom att manuellt kontrollera samtliga personposter i katalogen mot befolkningsregistret. Detta görs med ett egenutvecklat verktyg, NamePolicyControl, som jämför uppgiftena i katalogen med data i befolkningsregistret/Navet. Kontroll av skyddade personer med skyddet "Skyddad Folkbokföring" görs med hjälp av HSA Portalen. Om avvikelser påträffas korrigerar huvudadministratör uppgifterna utan godkännande av katalogadministratör. Kontrollen genomförs en gång per månad.

☒ Personer i HSA som hanteras av vår organisation har ett anställnings- eller uppdragsförhållande till den organisation de tillhör i HSA.

Detta säkerställer vi vid registrering av personer på följande sätt: katalogadministratör får i uppdrag att lägga upp personpost från ansvarig chef. Personposter under externa vårdgivare hanteras via ett eget formulär. Separat handlingsplan beskriver hur arbetet kommer att utföras.

För att verifiera att anställnings- eller uppdragsförhållandet kvarstår gör vi på följande sätt: Anställningsförhållande verifieras genom manuell kontroll mot personalsystemet en gång per kvartal. Lista över anställda hämtas från personalsystemet. Konsulter läggs upp på beställning av uppdragsgivare. Som hjälp till verifiering av uppdragsförhållande används attributet tom-datum. Undantag kan beviljas om annan rutin säkerställer att personposter inte riskerar att liggande. Externa vårdgivare redovisas i separat handlingsplan. Kontrollen genomförs av huvudadministratör.

Välj ett av de tre nedanstående alternativen.

☐ Vi har inga studenter registrerade under vår organisation i HSA.

☐ Vi tillämpar samma periodicitet och metoder för verifiering av anställnings-/uppdragsförhållande för studenter som för andra medarbetare enligt beskrivning ovan.

☒ Vi verifierar anställnings-/uppdragsförhållande för studenter vid skapande samt terminsvis på följande sätt Studenter kontrolleras mot respektive lärosäte genom utbyte av listor varje termin.

På följande sätt verifierar vår organisation personuppgifter för personer som saknar svenskt personnummer eller samordningsnummer.

☒ När vår organisation registrerar personer som saknar svenskt personnummer eller samordningsnummer verifierar vi personuppgifter med hjälp av uppvisad identitetshandling (enligt definition i Informationsspecifikation Katalogtjänst HSA [2]). En kopia av identitetshandlingen arkiveras hos vår organisation. Identitetshandlingens nummer och giltighetstid registreras i HSA tillsammans med personens födelsedatum. Personobjektet i HSA har inte längre giltighetstid än identitetshandlingen.

4.2.2 Organisationsuppgifter

Välj ett av de två nedanstående alternativen.

☐ Vår organisation agerar inte HSA-ombud, d.v.s. registrerar inte information om någon annan organisation eller verksamhet som inte är vår egen.

☒ Vår organisation agerar HSA-ombud, och vi förbinder oss därför att verifiera organisationsuppgifter mot SCB:s och/eller Bolagsverkets register genom användning av organisationsnummer. Detta gör vi på följande sätt: Endast ett fåtal centrala administratörer kan lägga upp enheter. Vid beställning av upplägg av extern organisation kontrolleras alltid organisationsuppgifter mot www.solidinfo.se.
När vår organisation ska avsluta en organisation på organisationsnivå (o-nivå) i HSA kontaktar vi HSA Förvaltning för hjälp.

4.2.3 Vårdgivare och vårdenheter

☒ När vår organisation markerar en organisation eller enhet som vårdgivare i HSA verifierar vi först att organisationsnumret återfinns vid sökning mot Inspektionen för vård och omsorgs (IVO) Vårdgivarregister.

☒ De vårdenheter och verksamhetschefer som vår organisation har registrerat i HSA är korrekta och uppdaterade enligt vårdgivarens beslut.

☒ Vår organisation tar inte bort vårdgivare och vårdenheter ur HSA. De arkiveras istället i HSA. Om en vårdenhet byter vårdgivare arkiveras vårdenheten och en ny vårdenhet skapas.

☒ Vår organisation säkerställer att vi för arkiverade vårdgivare sparar namn, HSA-id, organisationsnummer samt eventuellt start- och slutdatum och att vi för arkiverade vårdenheter sparar namn, HSA-id, eventuellt start- och slutdatum samt vårdgivartillhörighet.

4.2.4 HSA-id

☒ I vår organisations HSA-information är alla objekt identifierade med HSA-id.

☒ Vår organisations HSA-id är uppbyggda enligt gällande syntax.

☒ När personer tas bort ur HSA sparar vår organisation alltid kopplingen mellan HSA-id och person-id. Detta säkerställer vi genom att personers id-nummer lagras i en databas och blir därmed unikt. Kopplingen mellan HSA-id och person-id sparas för alltid. Regionjurist och arkivarie bedömer att denna typen av information ska bevaras för arkivändamål i enligthet med GDPR, arkivlagen och riksarkivets föreskrifter. Vi säkerställer att uppgiften tas bort efter att arkiveringstiden gått ut genom <saknas>.

☒ Om en person byter personidentitet (t.ex. från samordningsnummer till personnummer) säkerställer vår organisation att HSA-id ej ändras. Vi skapar INTE personen på nytt så att den får ett nytt HSA-id. Undantag görs i känsliga fall som t.ex. byte av personidentitet på grund av hot och våld där koppling mellan tidigare och ny personidentitet saknas i befolkningsregistret.

Välj ett av de två nedanstående alternativen.

☒ Vid byte av personidentitet sparar vi inte den tidigare personidentiteten, inte ens i Limbo eller motsvarande struktur för inaktiva personer.

☐ Vid byte av personidentitet sparar vi den tidigare personidentiteten på följande sätt: [beskrivning av hur tidigare personidentitet sparas].

Vi sparar personidentiteten eftersom: [motivering till varför den tidigare personidentiteten sparas].

4.2.5 Särskilt tillstånd kring fingerade data i monitorerings- och verifieringssyfte

Välj ett av de två nedanstående alternativen.

☐ Vår organisation kommer inte att registrera eller använda fingerade data i HSA:s produktionsmiljö.

☒ Vår organisation har behov av att registrera och använda en begränsad mängd fingerade data i HSA:s produktionsmiljö i monitorerings- och verifieringssyfte. Dessa data kommer att användas enligt följande: 1) i samband med produktionssättning görs en extra kontroll av leverantören att viktiga funktioner fungerar 2) för leverantörens healthcheck kontroll dvs att katalogen är online och att tjänsten fungerar. 3) för att ansvariga för e-tjänster skall kunna testa nya funktioner innan de läggs ut i verksamheterna. 4) för test av IT-tjänster som saknar testmiljö. Testdata finns under grenen (ou) Övrigt - Test och utbildning. RA-funktionen säkerställer att inga certifikat blir utgivna till dessa personer 5) för att kunna administrera den lokala säkerhetstjänsten ges medarbetaruppdrag till en grupp anställd hos CGI, (ou) Enheten för spärradmin är skapad för detta syfte.

Fingerade data kommer endast att registreras i vår organisations delträd under ”o=Testdata i Produktionsmiljö” och hanteringen kommer att följa riktlinjerna för tester och testdata i HSA [6].

4.3 Krav på tillgänglighet

☒ Vi är medvetna om att vår organisation bör ha samma målsättning för tillgänglighet för vår lokala katalog eller motsvarande som gäller för HSA. Målsättningen är att HSA är tillgängligt dygnet runt under årets alla dagar. Detta ska vara utgångspunkten för såväl drift som applikationsutveckling av HSA.

☒ Om LDAP används vid kommunikation mot HSA följer vi HSA LDAP-policy [7].

4.4 Krav på spårbarhet

☒ Alla förändringar som görs i vår organisations lokala katalog eller motsvarande och som påverkar innehållet i vår HSA-information loggas.

☒ Loggningen sker på ett sådant sätt att all förändring av informationsinnehåll i HSA kan spåras.

☒ Loggfiler innehåller information om vilken förändring som gjorts, om användaren/systemet som gjorde förändringen och om tidpunkten för förändringen.

☒ Loggningen sker på ett sådant sätt att ansvarig administratör kan identifieras.

☒ Vår organisation har, med hänsyn till gällande lagstiftning, beslutat att loggfiler ska sparas i 5 år.

4.5 Krav på sekretess

☒ I vår organisations lokala katalog eller motsvarande kan information som kräver utökad behörighet endast registreras av och visas för behöriga administratörer.

☒ I vår organisations lokala katalog eller motsvarande regleras åtkomst till information i enlighet med HSA Informationsklassning [11].

☒ I vår organisation hanterar vi personer med skyddade personuppgifter på följande sätt:

Skyddade personer i vår organisation är dolda i HSA och kan endast hanteras av ett fåtal utsedda administratörer.

Personer med skyddade personuppgifter informeras av närmsta enhetschef/verksamhetschef eller central katalogadministratör om hur personuppgifterna hanteras.

Kontroller av nytillkomna och borttagna skyddade personuppgifter hanteras via de regelbundna kontrollerna mot befolkningsregistret som beskrivs i avsnitt 4.2.1.

Välj ett av de två nedanstående alternativen.

☒ Personer med skyddade personuppgifter kan välja om uppgifterna ska göras synliga genom att kontakta utsedd personalhandläggare eller central katalogadministratör.

☐ I vår organisation tillåter vi inte att personer med skyddade personuppgifter görs synliga.

Välj ett av de två nedanstående alternativen.

☒ All kommunikation mot vår lokala katalog är krypterad.

☐ Kommunikation med interna källsystem sker okrypterat över organisationsinterna nätverk i följande fall: [Förteckning över samtliga informationsutbyten som sker okrypterat].

Vår bedömning är att säkerheten ändå kan anses garanteras eftersom: [beskrivning av hur säkerheten säkerställs].

4.6 Kontinuitetsplanering

☒ Vår organisation ansvarar för egen kontinuitetsplanering i händelse av störningar i HSA. Vi är medvetna om att vår organisation bör dokumentera kontinuitetsplanen för HSA.

4.7 Säkerhetskopiering

☒ Vår organisation säkerhetskopierar information i vår lokala katalog eller motsvarande regelbundet, minst en gång per dygn om förändringar av informationsinnehåll gjorts.

☒ Säkerhetskopiorna förvaras åtskilt från den lokala katalogen eller motsvarande.

4.8 Skydd mot intrång

☒ Vår organisation skyddar vår lokala katalog eller motsvarande 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 är begränsat till personal med särskild behörighet. Detaljerad beskrivning av behörighetsregler och procedurer för tillträde är dokumenterat.

4.9 Styrning av åtkomst

☒ Åtkomst till information i vår lokala katalog eller motsvarande föregås av autentisering direkt av individ eller indirekt via annat system.

☒ Behörigheter till olika informationsmängder i vår lokala katalog eller motsvarande är reglerad i enlighet med HSA Informationsklassning [11].

4.9.1 Styrning av åtkomst för HSA-administratörer

☒ Vår organisation utser administratörer samt lägger till och tar bort administratörsrättigheter enligt beskrivning i bilaga 1.

☒ Administratörer av vår lokala katalog identifierar sig med stark autentisering. Vi använder SITHS certifikat.

4.9.2 Styrning av åtkomst för konsument

Ej tillämplig för HPT Producent.

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

[Utrymme för egna refererade dokument]

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.

<saknas>

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

Bilagor

Nedan redovisas vilka bilagor som finns till HPT Producent.

Bilaga 1: Lokal organisation för administration av uppgifter som publiceras i HSA

Bilaga 2: Beskrivning av organisationens anrop mot HSA

Bilaga 1 Lokal organisation för administration av uppgifter som publiceras i HSA

Denna bilaga beskriver hur den lokala organisationen för administration av information i HSA ser ut vad gäller roller och ansvarsfördelning samt rutiner för behörighetshantering.

Om organisationen agerar HSA-ombud ska beskrivningarna nedan även omfatta tredjepartsanslutna organisationers förhållanden.

Roller och ansvarsfördelning

Vår lokala HSA-förvaltning består av följande roller med följande ansvar:

- HSA-ansvarig, utses av chefen för Området för Krisberedskap Säkerhet och Miljöledning
- Ställföreträdande HSA-ansvarig, utses av HSA-ansvarig
- Andra HSA-administratörer, utses av förvaltningsledning eller HSA-ansvarig enligt särskilt regelverk
- För att säkerställa att HSA-administration alltid kan hanteras när det behövs i vår organisation gör vi på följande sätt: den central katalogadministrationen är alltid bemannad på kontorsarbetstid. Beskrivningen avser uppdatering i lokal katalog

<saknas>

Rutiner för behörighetshantering

Administratörsbehörigheter i HSA läggs till och tas bort av person med rollen utökad katalogadministratör i vår lokala katalog.

Den som lägger till och tar bort administratörsbehörigheter får veta när administratörer slutar och börjar genom att: Nya katalogadministratörer registreras efter att en beställningsblankett signerad av ansvarig chef skickats in. När en person med behörighet som katalogadministratör flyttas eller tas bort från katalogen visas en påminnelseavisering om att behörigheterna finns och ska avbeställas.

Lokal katalog eller motsvarande för uppdatering av HSA-information

Information i detta avsnitt är inte reglerat i policyn och förändringar i dessa förutsättningar innebär därför inga krav på uppdatering av HPT. Informationen samlas in för att kunna ge en heltäckande och översiktlig bild av administrationen och informationsflödet för HSA.

Vår organisation uppdaterar HSA från Skånekatalogen, lokal HSA katalog med egna anpassningar. Databasen består av ett Microsoft AD. Informationen administreras via ett administrationsgränssnitt mot denna lokala katalog eller motsvarande av cirka 900 lokala administratörer.

Vår interna katalog eller motsvarande föds också från följande källor (utöver befolkningsregister och HOSP):

HR-system, (befattningskoder, chefskoder) Exchange systemet (e-postadresser)

Bilaga 2 Beskrivning av organisationens anrop mot HSA

Denna bilaga beskriver organisationens anrop som görs mot HSA för att hämta och/eller skriva information. Syftet med bilagan är att utgöra beslutsunderlag för HSA Policygrupp vid ny eller förändrad anslutning, men också att kunna användas som underlag för beskrivning av organisationens (inklusive tredjepartsanslutna) nyttjande av HSA samt som underlag vid utredningar om framtida förändringar i HSA, avseende påverkan av förändringar i informationsspecifikation och nationellt förvaltade gränssnitt samt dimensionering av produktionsmiljön.

Synkronisering från lokal katalog till HSA

Om ingen synkronisering från lokal katalog sker – sätt streck i samtliga grå fält och lämna kryssrutorna tomma.

Vi använder följande verktyg för synkronisering från lokal katalog till HSA:

Tieto, hanterar drift/utveckling av Microsoft Indentity Manager

Vår synkanvändare för produktionsmiljö är:

cn=rsMIM_Meta,ou=Users,o=Security,o=Region_Skane,dc=Nod1,dc=Services,c=SE
cn=rsFimMeta,ou=Users,o=Security,o=Region_Skane,dc=Nod1,dc=Services,c=SE

Välj ett av de två nedanstående alternativen.

- ☒ Vår synkronisering från lokal katalog till HSA följer HSA LDAP-policy [7].
- ☐ Vår synkronisering från lokal katalog till HSA följer HSA LDAP-policy [7] förutom i följande fall: [kortfattad beskrivning av avvikelse(r)].

  Denna/dessa avvikelse(r) avser vi åtgärda på följande sätt: [kortfattad beskrivning av de åtgärder som planeras].

  Åtgärderna planerar vi ha vidtagit senast [tidpunkt].

Vår synkronisering från lokal katalog till HSA kan beskrivas på följande övergripande sätt:

Inkrementell synkronisering (löpande modifiering, d.v.s. skapande, ändring, flytt och borttag av enskilda objekt) görs Frekvensen för synk är var 15:e minut. I genomsnitt görs cirka 60 modifieringar per timme.

Fullständig synkronisering (totalsynk) görs fullexport 18:45 varje dag.

Totalt omfattas ca 85000 objekt av vår synkroniseringsprocess.

Källan för den information i HSA som vi publicerar kan beskrivas på följande översiktliga sätt. Alternativet Hanteras ej betyder att informationsmängden inte alls finns i HSA för vår organisation.

Informationsmängd	Hanteras ej	Via synk	Annat
Organisationsstruktur	☐	☒	☐ nämligen [ange verktyg eller beskriv kortfattat]
Enheters kontakt-, verksamhets- och presentationsinformation	☐	☒	☐ nämligen [ange verktyg eller beskriv kortfattat]
Vårdgivarstruktur, medarbetaruppdrag enligt PDL,	☐	☒	☐ nämligen [ange verktyg eller beskriv kortfattat]
Administrativa medarbetaruppdrag	☐	☐	☒ nämligen Via Hau
Grunduppgifter anställda	☐	☒	☐ nämligen [ange verktyg eller beskriv kortfattat]
Grunduppgifter medarbetare hos externa uppdragstagare	☐	☒	☐ nämligen [ange verktyg eller beskriv kortfattat]
Grunduppgifter personer med skyddade personuppgifter	☐	☒	☐ nämligen [ange verktyg eller beskriv kortfattat]
Grunduppgifter personer utan person- eller samordningsnummer	☐	☒	☐ nämligen [ange verktyg eller beskriv kortfattat]
Anställnings-/uppdragsrelaterad information (t.ex. befattning, individuell egenskap för it-tjänster)	☐	☒	☐ nämligen [ange verktyg eller beskriv kortfattat]
HOSP-uppgifter (legitimation, specialistkompetens m.m.)	☐	☒	☐ nämligen [ange verktyg eller beskriv kortfattat]
Kontaktuppgifter personer	☐	☒	☐ nämligen [ange verktyg eller beskriv kortfattat]

Synkronisering från HSA till lokal katalog

Om ingen synkronisering från HSA till lokal katalog sker – sätt streck i samtliga grå fält och lämna kryssrutorna tomma.

Vi använder följande verktyg för synkronisering från HSA till lokal katalog:

cn=rsMIM_Meta,ou=Users,o=Security,o=Region_Skane,dc=Nod1,dc=Services,c=SE
cn=rsFimMeta,ou=Users,o=Security,o=Region_Skane,dc=Nod1,dc=Services,c=SE

Tieto

Välj ett av de två nedanstående alternativen.

☒ Vår synkronisering från HSA till lokal katalog följer HSA LDAP-policy [7].

☐ Vår synkronisering från HSA till lokal katalog följer HSA LDAP-policy [7] förutom i följande fall: [kortfattad beskrivning av avvikelse(r)].

Denna/dessa avvikelse(r) avser vi åtgärda på följande sätt: [kortfattad beskrivning av de åtgärder som planeras].

Åtgärderna planerar vi ha vidtagit senast [tidpunkt].

Vår synkronisering från HSA till lokal katalog kan beskrivas på följande övergripande sätt:

Inkrementell synkronisering (löpande modifiering, d.v.s. skapande, ändring, flytt och borttag av enskilda objekt) görs [Frekvensen för synk är var 15:e minut]. I genomsnitt görs cirka 45 modifieringar per timme.

Fullständig synkronisering (totalsynk) görs full import Hsa kl 04:40 varje dag,.

Totalt omfattas ca 85000 objekt av vår synkroniseringsprocess.

Följande informationsmängder hämtar vi från HSA till lokal katalog via vår synkronisering:

Informationsmängd	Ja	Nej
Kort- och certifikatinformation	☒	☐
HOSP-information för synkronisering med intern katalog	☒	☐

HSA kodverk	☐	☒
Uppgifter om verksamheter och/eller medarbetare i andra organisationer (kräver avtal)	☐	☒
Annat, nämligen [beskriv översiktigt den/de övriga informationsmängder som hämtas från HSA till den lokala katalogen]	☐	☒

Övriga anrop mot HSA

Beskriv övriga anrop som görs mot HSA, t.ex. tjänstekontrakts- eller WebService-anrop från lokala tjänster eller (o)regelbundna manuella kvalitetskontroller via LDAP-browser. Om inga andra anrop görs mot HSA – sätt streck i samtliga grå fält på översta raden.

Metod och systemanvändare	Sökbas	Sökfilter	Attribut i söksvar	Frekvens	Användning av sökresultat
[LDAP-fråga från cn=rsHospUser, ou=Hosp, o=Region_Skane, dc=Nod1,dc=Services,c=SE]	[dc=Hosp, dc=Services, c=se]	personalIdentityNumber=%)	personalIdentityNumber=%)	ca 50 ggr/dag under kontorstid, maxbelastning inträffar 19:00 varje dag med ca 60000 anrop	[Upplägg av anv i lokalt kataloggränssnitt]
[LDAP-fråga från cn=rsHospUser, ou=Hosp, o=Region_Skane, dc=Nod1,dc=Services, c=SE]	dc=Hosp, dc=Services, c=se	(&(!(deletedDate=*)) (objectClass=person) (mainNode=Ja))	cn, personalPrescriptionCode, specialityCode, specialityName, hsaTitle,hsaSosRestrictionsCode, hsaSosRestrictions, hsaSosEducationCode,	Varje dag kl 10:00, månd. - lörd	Uppdatering av HOSP-data för samtliga personer under o=Region

			hsaSosTitleCode, hsaSosNursePrescriptionRight		Skåne (ca 47000)
[HSAWS: GetCareUnit cn=Saktjanster.i.skane.se,ou=Applikationer, o=Region_Skane,dc=Nod1,dc=Services,c=SE]				< 10 anrop i veckan	Anropas av säkerhetstjänsterna. Utnyttjas ännu inte regelbundet.
[HSAWS: GetCareUnitList cn=Saktjanster.i.skane.se,ou=Applikationer, o=Region_Skane,dc=Nod1,dc=Services,c=SE]				< 10 anrop i vecka	Anropas av säkerhetstjänsterna. Utnyttjas ännu inte regelbundet
[HSAWS: GetHsaPerson cn=Saktjanster.i.skane.se,ou=Applikationer, o=Region_Skane,dc=Nod1,dc=Services,c=SE]				< 10 anrop i vecka	Anropas av säkerhetstjänsterna. Utnyttjas ännu inte regelbundet
[HSAWS: GetHsaUnit cn=Saktjanster.i.skane.se,ou=Applikationer, o=Region_Skane,dc=Nod1,dc=Services,c=SE]				< 10 anrop i vecka	Anropas av säkerhetstjänsterna. Utnyttjas ännu inte regelbundet

HSAWS: GetMiuForPerson cn=Saktjanster.i.skane.se,ou=Applikationer, o=Region_Skane,dc=Nod1,dc=Services,c=SE]				< 10 anrop i vecka	Anropas av säkerhetstjänsterna. Utnyttjas ännu inte regelbundet
[HSAWS: Ping cn=Saktjanster.i.skane.se,ou=Applikationer, o=Region_Skane,dc=Nod1,dc=Services,c=SE WS: Ping]				< 10 anrop i vecka	Anropas av säkerhetstjänsterna. Utnyttjas ännu inte regelbundet
[LDAP-frågor med t ex Apache Directory Studio]	o=Region Skåne,l=Skåne län,c=SE			ca. 10 per dag	Manuella kontroller. Exempel: Efterfråga all information om ett objekt. Lista alla personer i ett delträd
Tjänstekontraktsanrop getEmployeeIncludingProtectedPerson, Mina Planer	l=Skåne län, c=SE			200 gånger per timme (max 180 000 gånger per timme, nattetid)	Sammanhållen vårdplanering
Fileservice hsaUnitsExtended, Mina Planer	l=Skåne län,c=SE			Endast 1 gång nattetid	sammanhållen vårdplanering
