HSA Tillitsramverk

inera
Ett företag inom SKR

Innehållsförteckning

Kontaktuppgifter

Detta tillitsramverk förvaltas av Inera AB. Frågor, synpunkter och förslag rörande tillitsramverket 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
5.0	2024-05-03	***HSA Tillitsramverk 5.0 fastställdes av HSA Policygrupp 2024-05-03, efter remissförfarande. Tillitsramverket gäller från och med 2025-01-01. Följande ändringar är gjorda jämfört med HSA-policy 4.2.*** **Utifrån krav från E-hälsomyndigheten för åtkomst till nationella läkemedelslistan har följande bör-krav med krav på redogörelse av efterlevnad införts. Dessa krav är försedda med tillägget: "Att inte uppfylla ovanstående krav kan medföra att organisationens medarbetare inte ges åtkomst till skyddsvärd information i tjänster som använder HSA som källa för den behörighetsgrundande informationen."** • *(avsnitt 2.1) Ny roll HSA Säkerhetsansvarig med uppgift att genomföra personkontroller av HSA-ansvarig och ställföreträdande samt att initiera och följa upp internrevisioner.* • *(nytt avsnitt 2.2) Krav på personkontroller för HSA-ansvarig och ställföreträdande samt för medarbetare hos Inera eller Ineras leverantörer. Till detta även ett nytt styrande dokument "Instruktion för bakgrundskontroll enligt HSA Tillitsramverk".* • *(avsnitt 2.3.3, tidigare 2.2.3) Krav på inlämning av ny tillitsdeklaration minst vartannat år, oavsett om förändring skett eller inte.* • *(avsnitt 2.9, tidigare 2.7) Krav att internrevision ska utföras av oberoende part.* • *(avsnitt 4.1) Särskilda krav på hur organisationens informationssäkerhetsarbete ska bedrivas.* **Övriga ändringar:** • *Namnbyte på regelverket från HSA-policy till HSA Tillitsramverk. Som konsekvens byts även begreppet HSA-policytillämpning (HPT) mot begreppet HSA Tillitsdeklaration.* • *Tillägg av det styrande dokumentet "Eskaleringsprocess vid allvarliga avvikelser mot HSA Tillitsramverk".* • *Förtydligat att informationsklassning även finns för tjänstens it-komponenter.* • *Infört beskrivning av anslutningsformen HSA Tillitsdeklaration för konsument Behörighetsområde.* • *Förtydligat att samtliga krav i tillitsramverket gäller samtliga anslutna oavsett anslutningsform.* • *Ändrat krav att anmäla ställföreträdande från bör- till ska-krav.* • *Begreppet HSA Förvaltning ersatt med HSA Policygrupp (som ställer krav och följer upp enligt regelverket) och Inera (som är avtalsparten).* • *Tillagt krav att även konsumenter ska anpassa till gällande schema*

- *Tillagt krav att upphöra med anrop mot gränssnitt, metod eller version av metod för konsumtion av HSA-information inom 18 månader från meddelat end-of-life.*
- *Nytt avsnitt som beskriver vad som händer om tjänsten HSA upphör.*
- *Förtydligade krav på att förändringar ska göras när de blir kända och att regelbunden verifiering av informationsinnehållet ska genomföras.*
- *Förtydligad frekvens för kontroll av anställnings- och uppdragsförhållande, med max 100 dagars mellanrum istället för varje kvartal.*
- *Förtydligat krav om hur kontroll av anställnings- och uppdragsförhållande ska beskrivas i HSA Tillitsdeklaration för producent.*
- *Förtydligat krav för kontroll av behörighetsgrundande information i nytt avsnitt.*
- *Tillagt möjlighet att redovisa om organisation har annan kontrollmyndighet än Inspektionen för vård och omsorg.*
- *Tillagt krav att HSA-id endast ska kunna ändras av ett fåtal personer i lokal katalog (på samma sätt som det fungerar i den nationella katalogen)*
- *Mindre språkliga justeringar och förtydliganden.*
- *Uppdatering och förtydliganden av referenser.*

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 ett nationellt tillitsramverk och tillhörande styrande dokument. Organisationer verksamma inom vård och omsorg kan välja att ansluta till HSA och ansvarar då för att samtliga krav i tillitsramverket efterlevs.

Anslutna organisationer kan utgöra producenter och/eller konsumenter av HSA-information. Varje ansluten organisation tar fram och förvaltar en HSA Tillitsdeklaration som beskriver hur organisationen uppfyller HSA Tillitsramverk.

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.
- informationen i HSA ska följa vid var tid gällande schema och värdemängder.
- informationen ska förvaltas så att innehållet är uppdaterat och korrekt.
- internrevision av efterlevnad till HSA Tillitsramverk görs med max 13 månaders mellanrum.
- - vid uppdatering av HSA från lokal katalog eller motsvarande - konfidentialitet, riktighet, tillgänglighet och spårbarhet säkerställs i den lokala tjänsten.

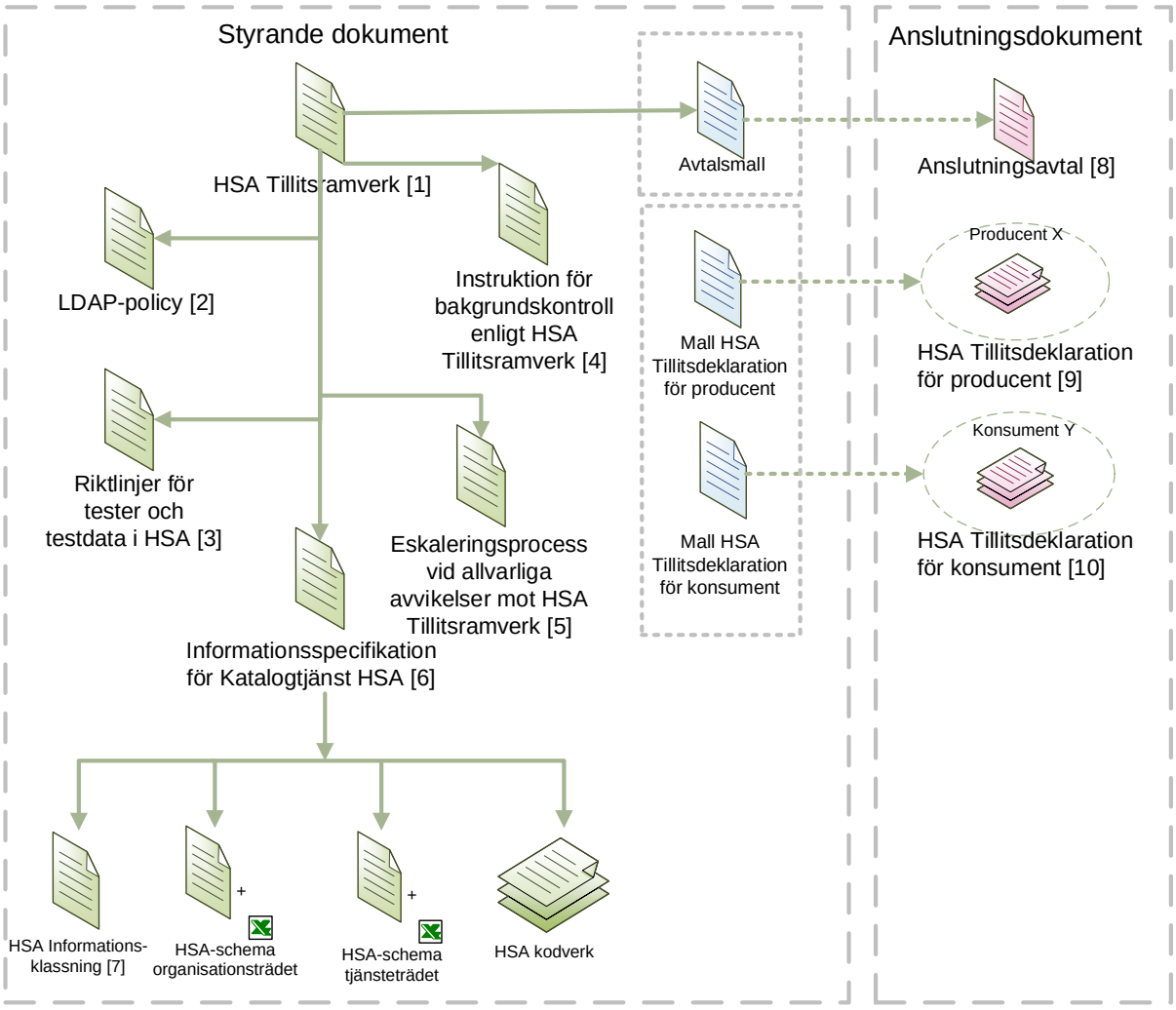
De krav som ställs på konsumenter av HSA-information är bland annat att:

- en kontaktperson utses som praktiskt ansvarar för organisationens anslutning.
- informationen från HSA endast får användas på det sätt som är beskrivet i tillitsdeklaration godkänd av HSA Policygrupp.
- internrevision av efterlevnad till HSA Tillitsramverk görs med max 13 månaders mellanrum.
- kontinuitetsplanering finns för den händelse att HSA ej är tillgänglig.
- 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 Tillitsramverk 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 Tillitsramverk [1]** (detta dokument), ett styrande dokument för HSA på övergripande nivå.
- **LDAP-policy [2]** beskriver hur kommunikation via LDAP ska ske mot HSA.
- **Riktlinjer för tester och testdata i HSA [3]**, beskriver hur tester och testdata hanteras samt vilka regler som gäller för registrering och hantering av fingerade uppgifter.
- **Instruktion för bakgrundskontroll enligt HSA Tillitsramverk [4]**, beskriver hur bakgrundskontroll ska genomföras för att godkännas som uppfyllelse av kravet om bakgrundskontroll.

- **Eskaleringsprocess vid allvarliga avvikelser mot HSA Tillitsramverk [5]**, beskriver den process för eskalering som tillämpas då en ansluten organisation (producent eller konsument) bryter mot HSA Tillitsramverk.
- **Informationsspecifikation för Katalogtjänst HSA [6]**, beskriver informationsinnehållet i HSA. Till detta dokument finns följande bilagor:
    - HSA Informationsklassning [7], som beskriver klassning av HSA-informationen och tjänstens it-komponenter ur konfidentialitets-, riktighets-, tillgänglighets- och spårbarhetssynpunkt
    - HSA-schema, organisationsträdet
    - HSA-schema, tjänsteträdet
    - HSA kodverk, som beskriver tillåtna värden för vissa attribut
- **Anslutningsavtal [8]**, baserat på Ineras kundavtal med tillhörande bilagor, tecknas mellan Inera AB och producenten respektive konsumenten och reglerar ansvarsfördelningen mellan parterna.
- **HSA Tillitsdeklaration för producent [9]**, skrivs av varje organisation som publicerar (tillgängliggör) information till HSA och beskriver hur den enskilda organisationen uppfyller kraven i HSA Tillitsramverk. Det finns en särskild variant av tillitsdeklaration som är framtagen för de organisationer som endast använder det nationellt förvaltade administrationsgränssnittet för att uppdatera information i HSA manuellt.
- **HSA Tillitsdeklaration för konsument [10]**, skrivs av organisationer som använder (hämtar) information från HSA såsom konsument och beskriver hur organisationen uppfyller kraven på informationshantering i HSA Tillitsramverk. Det finns två särskilda varianter av tillitsdeklaration som är framtagna för de organisationer som endast hämtar publik enhetsinformation respektive för de organisationer som har ansvar för ett eller flera behörighetsområden i HSA, men som inte konsumerar HSA-information direkt från HSA.

1 Introduktion

1.1 Översikt

Detta dokument utgör ett nationellt tillitsramverk för HSA. Tillitsramverket 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 detta tillitsramverk är en förutsättning för att vara ansluten till HSA.

Tillitsramverket förvaltas av Inera AB och fastställs av HSA Policygrupp.

Direktanslutna organisationer, såväl producerande organisationer (producenter) som konsumerande organisationer (konsumenter), bekräftar efterlevnad av detta tillitsramverk genom anslutningsavtal och upprättande av en HSA Tillitsdeklaration, som godkänns av HSA Policygrupp.

Alla krav i tillitsramverket gäller alla anslutna organisationer, oavsett anslutningsform. Kraven gäller också HSA Förvaltning och HSA Policygrupp. Beroende på anslutningsform är det emellertid i vissa fall inte möjligt att bryta mot enskilda krav. I dessa fall krävs inte någon redogörelse för att – och hur – kravet efterlevs. Vilka dessa krav är framgår i mallen för tillitsdeklaration för respektive anslutningsform.

1.2 Begrepp och definitioner

Definitioner av begrepp som används i detta tillitsramverk finns i särskilt dokument [11].

Tvingande krav för anslutna producenter och konsumenter anges i detta tillitsramverk 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 Tillitsramverk

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 Tillitsramverk 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 detta tillitsramverk, utöver HSA Policygrupp, är HSA-ansvariga och beslutsfattare hos anslutna producerande organisationer (producenter) samt kontaktpersoner och beslutsfattare hos anslutna konsumerande organisationer (konsumenter).

Tillitsramverket är tillämpbart för etablering, drift och förvaltning av HSA samt för användning av information från HSA.

2 Allmänna förutsättningar

Med ”direktansluten organisation” avses organisation (producent eller konsument) som har eget avtal med Inera omfattande användning av tjänsten HSA.

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.

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 till exempel tjänstekontrakt är bara tillåtet vid fullständig anslutning.

Med ”konsumerande organisation” och synonymen ”konsument” avses organisation som avseende en viss tjänst nyttjar information från HSA utan att egen information tillgängliggörs i HSA. Begreppet omfattar således både direktansluten och tredjepartsansluten konsument.

Det finns två huvudsakliga anslutningsformer för konsument, fullständig eller förenklad. Den senare innebär att konsumenten bara får läsa publik enhets- och funktionsinformation enligt särskild specifikation. Därutöver finns en särskild konsumentanslutning för de organisationer som har ansvar för ett eller flera behörighetsområden i HSA, men som inte konsumerar HSA-information direkt från HSA.

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 (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 (till exempel semester). HSA-ansvarig **ska** anmäla ställföreträdande HSA-ansvarig till Inera för att denna person ska ges samma rättigheter som HSA-ansvarig.

Direktansluten producent **bör** utse en HSA Säkerhetsansvarig, vars uppgift är att utvärdera organisationens efterlevnad av HSA Tillitsramverk genom att initiera samt följa upp resultat och åtgärdsplaner från internrevisioner och riskanalyser och att genomföra personkontroll för HSA-ansvarig och ställföreträdande HSA-ansvarig. Rollen som HSA Säkerhetsansvarig **får ej** kombineras med annan roll inom organisationens HSA-förvaltning. HSA-ansvarig **ska** anmäla utsedd HSA Säkerhetsansvarig till Inera.

Att inte uppfylla ovanstående krav kan medföra att organisationens medarbetare inte ges åtkomst till skyddsvärd information i tjänster som använder HSA som källa för den behörighetsgrundande informationen.

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 Personkontroller

2.2.1 Identitetskontroll

Innan en person tilldelas rollen HSA Säkerhetsansvarig **ska** HSA-ansvarig genomföra en identitetskontroll med hjälp av godkänd id-handling (enligt definition i Informationsspecifikation Katalogtjänst HSA [6]).

HSA Policygrupp har rätt att kräva att förnyad identitetskontroll genomförs.

2.2.2 Bakgrundskontroller

Bakgrundskontroller **bör** genomföras för personer som innehar eller ska tilldelas rollen HSA-ansvarig eller ställföreträdande HSA-ansvarig. Bakgrundskontroller **ska** genomföras av HSA Säkerhetsansvarig. Syftet med bakgrundskontroller är att förvissa sig om att personen kan anses

vara pålitlig och har de kvalifikationer och den utbildning som krävs för att på ett tillfredsställande, korrekt och säkert sätt utföra de arbetsuppgifter som följer av rollen.

Att inte uppfylla ovanstående krav kan medföra att organisationens medarbetare inte ges åtkomst till skyddsvärd information i tjänster som använder HSA som källa för den behörighetsgrundande informationen.

Kravet på bakgrundskontroll **ska** även omfatta medarbetare hos Inera eller Ineras leverantörer med behörighet att:

- lägga beställningar för förändringar i HSA.
- genomföra ändringar i andra organisationers HSA-information.

Genomförda bakgrundskontroller **ska** omfatta:

- identitetskontroll med hjälp av godkänd id-handling (enligt definition i Informationsspecifikation Katalogtjänst HSA [6]).
- nuvarande anställning.
- lämplighet för tjänsten.
- legal lämplighet.
- finansiell lämplighet.
- relevant utbildning.

Bakgrundskontroller **ska** genomföras enligt vid var tid aktuell Instruktion för bakgrundskontroll enligt HSA Tillitsramverk [4].

HSA Policygrupp har rätt att begära att förnyad bakgrundskontroll genomförs.

2.3 Förpliktelser för producerande organisation

2.3.1 Allmänt

Ansluten producent **ska** arbeta enligt detta tillitsramverk och garantera att organisationen till fullo uppfyller samtliga krav i tillitsramverket.

2.3.2 Förpliktelser för HSA-ansvarig hos direktansluten producerande organisation

För att inneha rollen som HSA-ansvarig **ska** personen ha 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 Tillitsramverk.
- det finns en kontinuitetsplan (avbrotts- och katastrofplan).
- det finns ett dokumenterat regelverk för hur administratörer utses och för hur behörigheter tilldelas.
- information från HSA Policygrupp och HSA Förvaltning på Inera sprids inom organisationen inklusive eventuella tredjepartsanslutna organisationer.
- LDAP-policyn för HSA [2] följs.
- Riktlinjer för tester och testdata i HSA [3] följs.
- personer med rättigheter att administrera organisationens HSA-information har kännedom om och arbetar i enlighet med HSA Tillitsramverk och godkänd HSA Tillitsdeklaration.
- aktuella kontaktuppgifter till HSA-ansvarig, ställföreträdande HSA-ansvarig och i förekommande fall HSA Säkerhetsansvarig 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.

2.3.3 HSA Tillitsdeklaration för producent

Direktansluten producent **ska** ta fram ett särskilt dokument, ”HSA Tillitsdeklaration för producent” [9], som beskriver hur detta tillitsramverk tillämpas. Framtagen tillitsdeklaration **ska** godkännas av HSA Policygrupp.

Tillitsdeklarationen **ska** utformas enligt anvisningarna i ”Mall HSA Tillitsdeklaration för producent”. All användning av HSA **ska** dokumenteras i tillitsdeklarationen.

Om någon förändring sker som påverkar innehållet i en direktansluten producents tillitsdeklaration **ska** ny tillitsdeklaration inlämnas skyndsamt. Den nya versionen **ska** baseras på aktuell mallversion.

Ny tillitsdeklaration **bör** inlämnas inom 24 månader från det att den senaste tillitsdeklarationen godkändes av HSA Policygrupp, oavsett om förändring skett eller inte.

Att inte uppfylla ovanstående krav kan medföra att organisationens medarbetare inte ges åtkomst till skyddsvärd information i tjänster som använder HSA som källa för den behörighetsgrundande informationen.

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

2.4 Förpliktelser för konsumerande organisation

2.4.1 Allmänt

Konsument **ska** arbeta enligt detta tillitsramverk 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.

2.4.2 Förpliktelser för kontaktperson hos konsumerande organisation

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

- informationshanteringen sker i enlighet med HSA Tillitsramverk och godkänd HSA Tillitsdeklaration.
- behandling av personuppgifter följer EU:s dataskyddsförordning (GDPR).
- - om personuppgifter från HSA hanteras i tjänsten – regelbunden teknisk uppföljning av aktuell säkerhetsnivå, till exempel 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 [3] efterlevs.
- personer som arbetar med HSA-information inom tjänsten (även inkluderat medarbetare hos eventuella underleverantörer) har kännedom om och arbetar i enlighet med HSA Tillitsramverk och godkänd HSA Tillitsdeklaration.
- 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 Policygrupp och HSA Förvaltning på Inera samt andra intressenter inom HSA.

2.4.3 HSA Tillitsdeklaration för konsument

Konsumenten **ska** ta fram ett särskilt dokument, ”HSA Tillitsdeklaration för konsument” [10], som beskriver hur detta tillitsramverk tillämpas. Framtagen tillitsdeklaration **ska** godkännas av HSA Policygrupp.

Tillitsdeklarationen **ska** utformas enligt anvisningarna i dokumentet ”Mall HSA Tillitsdeklaration för konsument”.

HSA Tillitsdeklaration för konsument **ska** innehålla en redogörelse för vilken information som används och hur denna nyttjas.

Om någon förändring sker som påverkar innehållet i en direktansluten konsuments tillitsdeklaration **ska** ny policytillämpning inlämnas skyndsamt. Den nya versionen **ska** baseras på aktuell mallversion.

Ny tillitsdeklaration **bör** inlämnas inom 24 månader från det att den senaste tillitsdeklarationen godkändes av HSA Policygrupp, oavsett om förändring skett eller inte.

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

2.5 Särskilda förpliktelser för HSA-ombud

Såväl producenter som konsumenter kan agera HSA-ombud. En konsument kan bara agera ombud för en annan konsumerande organisation medan en producent kan agera ombud både för producerande och konsumerande organisationer.

Följande krav gäller för både producenter och konsumenter som agerar HSA-ombud:

HSA-ombud **ska** ansvara för sina tredjepartsanslutna organisationer, som om de gällde deras egen organisation, för allt som detta tillitsramverk omfattar. Det inkluderar även genomförande av internrevision.

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 Policygrupp eller HSA Förvaltning på Inera.

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

Följande krav gäller endast producenter som agerar HSA-ombud:

HSA Tillitsdeklaration för 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 egna objekt.

HSA-ombud **ska** tillse att tredjepartsanslutning endast sker av organisationer inom vård- och omsorgssektorn.

Följande krav gäller endast konsumenter som agerar HSA-ombud:

HSA Tillitsdeklaration för konsument **ska** innehålla en beskrivning av vilka tjänster som använder HSA-information genom konsumentens anslutning samt vilka eventuella tredjepartsanslutna organisationer som ansvarar för dessa tjänster.

2.6 Informationsinnehåll i HSA

Informationsinnehållet i HSA **ska** följa den specifikation som anges i aktuell ”Informationsspecifikation för Katalogtjänst HSA” [6] med tillhörande bilagor som specificerar innehåll i HSA.

Vid uppgradering av HSA-schemat **bör** ansluten producent utan dröjsmål anpassa den egna organisationens HSA-information så att gällande schema följs.

Ansluten konsument **bör** utan dröjsmål utvärdera om uppgradering av HSA-schema påverkar den egna eller tredjepartanslutna organisationers tjänster och i så fall anpassa tjänsten så att gällande schema följs.

Anpassningarna **ska** vara införda senast tre månader efter uppgradering av HSA-schemat.

2.7 Gränssnitt för konsumtion av HSA-information

Ansluten producent eller konsument som enligt godkänd HSA Tillitsdeklaration har åtkomst till gränssnitt för konsumtion av HSA-information **bör** utan dröjsmål anpassa sin tjänst till användning av senaste version av aktuell metod. Då Inera meddelat end-of-life för en metod eller för en version av en metod **ska** ansluten producent eller konsument upphöra att anropa denna version eller metod inom 18 månader.

2.8 Hantering av andra organisationers information

Ansluten producent **får ej** tillgängliggöra HSA-information från annan ansluten producent utanför den egna organisationen, till exempel genom publicering på Internet eller annan spridning av information till tredje part, såvida inte särskild överenskommelse finns med den informationsägande organisationen.

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

Information från HSA **får ej** användas i marknadsföringssyfte, om inte uttryckligt medgivande från informationsägande organisation finns.

Konsument **får ej** ta betalt för vidareförmedling av HSA-information till tredje part.

2.9 Revision

Direktansluten producerande och konsumerande organisation **ska** löpande, med max 13 månaders mellanrum, genomföra internrevision för att kontrollera efterlevnad av krav i detta tillitsramverk. 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 tillitsdeklarationens aktualitet och överensstämmelse med tillitsramverket kontrolleras.

Internrevisionen **bör** utföras av oberoende part, på så sätt att den initieras och följs upp av HSA Säkerhetsansvarig eller av särskild roll eller funktion inom organisationen med särskilt ansvar för intern granskning.

Att inte uppfylla ovanstående krav kan medföra att organisationens medarbetare inte ges åtkomst till skyddsvärd information i tjänster som använder HSA som källa för den behörighetsgrundande informationen.

Genomförda revisioner **ska** dokumenteras och dateras. Revisionsrapporten **ska** (minst) innehålla en beskrivning av vad revisionen omfattat, vilka som medverkat vid revisionen, resultatet av revisionen inklusive identifierade brister samt en åtgärdsplan med angivelse av tidpunkt då respektive brist ska vara åtgärdad samt vem som ansvarar för åtgärden.

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 Policygrupp eller HSA Förvaltning på Inera. Allvarliga brister som påträffas lokalt som riskerar att påverka andra anslutna producenter eller konsumenter **ska** omedelbart rapporteras till HSA Förvaltning på Inera.

HSA Policygrupp, eller av HSA Policygrupp utsedd tredje part, **får** genomföra revision av ansluten producent eller konsument för att kontrollera efterlevnad av detta tillitsramverk.

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 till exempel förändringar och tillägg i tillitsramverk, schema och regelverk samt nya anslutningar.

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 HSA Tillitsdeklaration för producent [9] och konsument tar fram HSA Tillitsdeklaration för konsument [10].
3. Granskning sker av HSA Tillitsdeklaration.
4. Resultatet av granskningen redovisas i HSA Policygrupp som tar ställning till godkännande.
5. När HSA Tillitsdeklaration är godkänd undertecknas anslutningsavtal.

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

3.3 Om tjänsten HSA upphör

Om Inera eller Ineras ägare beslutar att tjänsten HSA inte längre ska tillhandahållas **ska** Inera ansvara för att informationen i HSA raderas.

Innan informationen raderas **ska**

- direktanslutna konsumenter ges möjlighet att inkomma med begäran om undantag från kravet att radera HSA-information i tjänsten.
    - Konsumenten ansvarar för att
        - begäran om undantag görs inom utsatt tid.
        - beskriva hur informationen ska hållas uppdaterad över tid när HSA inte längre är tillgänglig.

    - Inera ansvarar för att
        - tillhandahålla riktlinjer och mallar kopplade till begäran och beslut om undantag från kravet att radera HSA-information.
        - fatta beslut om undantag från kravet att radera HSA-information i tjänsten i samråd med HSA Policygrupp eller berörda direktanslutna producenter.
- direktanslutna producenter ges möjlighet att begära tillgång till den information i HSA som de äger och ansvarar för. Detta omfattar även information om tredjepartanslutna organisationer.
    - Producenten ansvarar för att
        - begäran om utlämning görs inom utsatt tid.
    - Inera ansvarar för att
        - informationen överförs på ett säkert sätt.
        - informationen lämnas ut i, av Inera beslutat, elektroniskt bearbetningsbart format.

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 tre aspekterna konfidentialitet, riktighet och tillgänglighet. Detaljerad vägledning kring kraven i detta kapitel ges bland annat av Myndigheten för samhällsskydd och beredskaps föreskrifter och allmänna råd om statliga myndigheters informationssäkerhet [12] samt i internationella standards som ISO/IEC 27001 [13] och ISO/IEC 27002 [14].

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 [15].

Ansluten producent **bör** dessutom

- hantera informationssäkerheten baserat på principer i enlighet med ISO/IEC 27001 [13] eller motsvarande likvärdiga principer för ledning och styrning av informationssäkerhetsarbetet.
- ha fastställda processer och rutiner för riskhantering som omfattar förmåga att identifiera, analysera och motverka risker.

- ha en incident- och avvikelsehantering med en hög medvetenhet och förmåga att upptäcka, lindra eller förhindra skada och utreda incidenter och avvikelser kopplade till tjänsten samt ett regelverk för när, och rutiner för hur, vidarerapportering sker.

Att inte uppfylla ovanstående krav kan medföra att organisationens medarbetare inte ges åtkomst till skyddsvärd information i tjänster som använder HSA som källa för den behörighetsgrundande informationen.

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.

Det innebär att uppdatering **ska** göras så snart som möjligt efter att en förändring blir känd, men också att regelbunden verifiering av befintligt informationsinnehåll **ska** göras.

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

Information i beskrivningar och fritextfält **får ej** 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 Policygrupp eller HSA Förvaltning på Inera.

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. Undantag kan även beviljas om tjänsten HSA inte längre tillhandahålls, se avsnitt 3.3.

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. HSA Tillitsdeklaration för 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 löpande, med max 100 dagars mellanrum. Undantag kan göras för studerande som gör praktik hos organisationen, vars uppdragsförhållande får kontrolleras terminsvis, förutsatt att detta beskrivs i godkänd HSA Tillitsdeklaration för producent.

Tillitsdeklarationen **ska** innehålla en beskrivning av hur anställnings- och uppdragsförhållanden kontrolleras, såväl vid registrering som löpande med max 100 dagars mellanrum, för:

- organisationens egna anställda.
- organisationens uppdragstagare (konsulter, bemanningspersonal eller motsvarande).
- studerande som gör praktik hos organisationen.

Om organisationen agerar HSA-ombud **ska** tillitsdeklarationen också innehålla en beskrivning av hur anställnings- och uppdragsförhållande kontrolleras för motsvarande kategorier hos tredjepartsanslutna organisationer.

I det fall svenskt personnummer eller samordningsnummer saknas **ska** verifiering av personuppgifter ske med hjälp av uppvisad godkänd id-handling (enligt definition i Informationsspecifikation Katalogtjänst HSA [6]). En kopia av id-handlingen **ska** arkiveras hos organisationen. Id-handlingens nummer och giltighetstid **ska** registreras i HSA tillsammans med personens födelsedatum. Personobjektet i HSA **får ej** ha längre giltighetstid än id-handlingen.

4.2.2 Behörighetsgrundande information

Behörighetsgrundande information, det vill säga medarbetaruppdrag samt individuell egenskap för it-tjänster, för samtliga registrerade personer **ska** verifieras med max 13 månaders mellanrum. Avseende behörighetsgrundande information som ger åtkomst till patientdata är detta ett krav även i Socialstyrelsens föreskrifter HSLF-FS 2016:40, 4 kap 3 §.

4.2.3 Organisationsuppgifter

Vid skapandet av organisationsuppgifter **ska** dessa verifieras mot SCB:s och/eller Bolagsverkets register genom användning av organisationsnummer. HSA Tillitsdeklaration för 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 HSA Tillitsdeklaration.

4.2.4 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. Om organisationen eller någon tredjepartsansluten

organisation står under annan myndighets kontroll **ska** detta redovisas i HSA Tillitsdeklaration för producent.

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.

4.2.5 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 till exempel åtkomst till patientdata). Periodicitet, arkiveringstid och procedurer för arkivering **ska** beskrivas i HSA Tillitsdeklaration för producent.

Vid byte av person-id (till exempel från samordningsnummer till personnummer) **får ej** HSA-id ändras. Undantag **ska** göras i känsliga fall som till exempel. 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 ej** lagras i separat objekt, inte ens i Limbo eller motsvarande struktur för inaktiva personer.

Om HSA uppdateras från lokal katalog eller motsvarande **ska** möjligheten att ändra HSA-id begränsas till ett fåtal personer.

4.2.6 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 tillitsdeklaration.

Hanteringen av fingerade data **ska** följa riktlinjerna för tester och testdata i HSA [3].

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 [2] 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.

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 [12] och [14].

Loggfiler innehållande förändringar av HSA-information som lagras nationellt 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 **ska** organisationen själv besluta hur länge loggfiler ska sparas med hänsyn till gällande lagstiftning (såväl GDPR:s principer för lagringsminimering som lagstiftning kopplad till krav på spårbarhet för till exempel åtkomst till patientdata). Hur länge loggfiler sparas **ska** beskrivas i HSA Tillitsdeklaration för producent.

Historisk information per objekt lagras nationellt i två år. Historisk information används för att presentera ändringar per objekt samt för felsökning.

Ansluten producent som uppdaterar samtlig information i HSA från lokal katalog har rätt att få sin information exkluderad ur historikhanteringen. I sådant fall **ska** producenten själv ansvara för felsökning i samband med ändringar i HSA om behov för detta skulle uppstå. Hur producenten säkerställer att felsökning kan göras **ska** beskrivas i HSA Tillitsdeklaration för producent.

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 [7].

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 HSA Tillitsdeklaration för producent. 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 HSA Tillitsdeklaration för producent beskriva hur uppgifterna hanteras.

All kommunikation mot HSA **ska** vara krypterad i enlighet med RIV anvisning för kryptering [16].

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.

4.6 Kontinuitetsplanering

Ansluten producent och konsument **ska** ansvara 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 den driftmiljö där HSA-information finns.

Om HSA uppdateras från lokal katalog eller motsvarande ställs samma krav på den lokala tjänsten. För mer vägledning kring säkerhetskopiering se [12] och [14].

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 eller dylikt 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 av en konsument **ska** regelbunden teknisk uppföljning ske av aktuell säkerhetsnivå. Sådan uppföljning kan innefatta till exempel – men inte uteslutande

– 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 [12] och [14].

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 [7].

Om konsument använder behörighetsgrundande information från HSA **ska** behörighetsmodellen där informationen används beskrivas i HSA Tillitsdeklaration för konsument.

För mer vägledning kring styrning av åtkomst, se [12] och [14].

4.9.1 Styrning av åtkomst för HSA-administratörer

Detaljerad beskrivning av procedurer för behörighetshantering för administratörer **ska** dokumenteras och redovisas i HSA Tillitsdeklaration för producent.

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

Publika HSA-dokument återfinns på Ineras informationssidor om tjänsten. Konfidentiella dokument tillgängliggörs för HSA-ansvariga och kontaktpersoner på behörighetsstyrd särskild dokumentyta. Externa referenser kan sökas fram, i förekommande fall från de länkar som referensen innehåller.

[1] HSA Tillitsramverk

[2] HSA LDAP-policy (konfidentiell)

[3]	Riktlinjer för tester och testdata i HSA
[4]	Instruktion för bakgrundskontroll enligt HSA Tillitsramverk
[5]	Eskaleringsprocess vid allvarliga avvikelser mot HSA Tillitsramverk
[6]	Informationsspecifikation för Katalogtjänst HSA
[7]	HSA Informationsklassning (konfidentiell)
[8]	Anslutningsavtal, baserat på Ineras mall för kundavtal med tillhörande bilagor
[9]	HSA Tillitsdeklaration för producent, baserad på mall
[10]	HSA Tillitsdeklaration för konsument, baserad på mall
[11]	HSA Begrepp och definitioner
[12]	Myndigheten för samhällsskydd och beredskaps information på https://informationssakerhet.se (extern)
[13]	SS-EN ISO/IEC 27001:2023, Informationssäkerhet- Cybersäkerhet och integritetsskydd - Ledningssystem för informationssäkerhet – Krav (extern)
[14]	SS-EN ISO/IEC 27002:2022, Informationssäkerhet, cybersäkerhet och integritetsskydd – Kontroller av informationssäkerhetsåtgärder (extern)
[15]	HSLF-FS 2016:40 Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården
[16]	RIV Tekniska anvisningar - Kryptering på https://rivta.se (extern)

Förkortningar

HOSP	Socialstyrelsens register över legitimerad hälso- och sjukvårdspersonal
LDAP	Lightweight Directory Access Protocol
GDPR	Europaparlamentets och rådets förordning (EU) nr 2016/679. GDPR är förkortning för General Data Protection Regulation.
RIV	Riktlinjer för interoperabilitet i vården, förvaltas av Inera Arkitektur & Regelverk

Begrepp och definitioner finns beskrivna i särskilt dokument [11].