Förtydligande av HSA-policyns krav kring spårbarhet (avsnitt 4.4) avseende användarkonton för manuell administration

Våren 2020 genomförde HSA Förvaltning en aktivitet för att om möjligt få bort användningen av opersonliga administratörskonton med höga behörigheter i HSA. Detta för att alltid kunna härleda en ändring som görs av informationen i HSA till en enskild administratör. På så sätt kan vi säkerställa spårbarheten i HSA som beskrivs i HSA-policy, avsnitt 4.4:

*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.*

I samband med kommunikationen med berörda HSA-anslutna organisationer kring denna aktivitet har följande förtydligande tagits fram.

- HSA-policyns krav avseende spårbarhet och loggning gäller för både nationella HSA och lokala kataloger eller lokala system som agerar källa till HSA.
    - I de fall ändring av uppgifter sker i en lokal katalog och därefter synkroniseras till HSA visar loggningen i HSA endast att uppgifterna ändrats av en synkanvändare. Därför är det viktigt att loggningen av motsvarande ändring i den lokala katalogen möjliggör identifiering av ansvarig administratör.
- Användarkonton för manuell administration **ska** alltid vara knutna till en – och endast en – fysisk person för att uppnå spårbarhet vid förändringar i HSA-information enligt HSA-policy, avsnitt. 4.4.
    - Ett personligt superadministratörskonto **bör** utgöras av ett personobjekt
    - Ett personligt superadministratörskonto som utgörs av ett personobjekt **bör** vara knutet till personens ordinarie personpost i HSA genom att samma HSA-id och person-id anges på båda posterna och kanske även en seeAlso-länk till den ordinarie personposten. Därtill **kan** personobjektet som motsvarar superadministratörskontot även behöva innehålla personens kort- och certifikatuppgifter (om det krävs för att möjliggöra stark autentisering).
    - För ett personligt superadministratörskonto som utgörs av ett personobjekt **ska** namnuppgifterna vara uppdaterade mot befolkningsregistret, enligt HSA-policy, kap. 4.2.1. Det namnsättande attributet (cn) **kan** även kompletteras med ytterligare information.
    - Om det personliga superadministratörskontot inte utgörs av ett personobjekt **bör** namnet innehålla innehavarens namn enligt befolkningsregistret, och en rutin **bör** tas fram för att säkerställa att namnet är korrekt över tid.
        - Observera ska-kravet ovan på knytning till en fysisk person. Görs detta inte via namnet måste det göras på annat sätt.
    - Personliga superadministratörskonton **bör** placeras i organisationsstrukturen så att det är lätt för administratören att välja rätt konto vid inloggning i ett gränssnitt. Detta kan till exempel innebära att de personliga superadministratörskontona placeras under en enhet kallad ”Superadministratörskonton”.