Behörighetsmodell för vård och omsorg

Innehåll

Revisionshistorik

Version	Datum	Författare	Kommentar
1.0	2011-12-09	HSA Förvaltningsgrupp	Slutversion till CeHis
2.0	2012-08-20	HSA Förvaltningsgrupp	Behörighetsmodellen omarbetad så att den även omfattar administrativa uppdrag som inte styrs av Patientdatalagen. Godkänd av HSA Förvaltningsgrupp.
2.1	2019-04-23	HSA Behörighetsgrupp	Anpassning efter ny nomenklatur för administrativa medarbetaruppdrag. Dokumentet omstrukturerat i ett huvuddokument och två underbilagor (bilaga 1 Vårdmedarbetaruppdrag och Bilaga 2 Administrativa medarbetaruppdrag). Huvuddokumentet även namnändrat från Behörighetsmodell hälso- och

			sjukvården till Behörighetsmodell för vård och omsorg.
2.2	2019-06-05	Henrika Littorin, Ronny Nilsson	Hantering av remissynpunkter.
2.3	2019-06-17	Henrika Littorin	Uppdaterat efter behandling i HSA Policygrupp.
2.4	2019-07-02	Henrika Littorin	Uppdaterat efter behandling vid arbetsmöte Inera Arkitektur & Regelverk och HSA Behörighetsgrupp.
2.5	2019-08-09	Henrika Littorin	Ersatt bilder med inlagd SmartArt.
3.0	2019-08-29	HSA Policygrupp	Fastställd av HSA Policygrupp.
3.1 – remiss	2020-11-19	Henrika Littorin	Förtydligat att åtkomst inom ramen för sammanhållen journalföring endast är tillåtet i ändamålet ”Vård och behandling”. Förtydligat att omfång ej kan sättas till enskilda enheter så länge aktiviteten är ”Läsa”. Lägsta nivå är vårdenhet. Justerat referenser.
3.1	2021-01-21	-	Godkänd av HSA Policygrupp
3.1.1	2021-03-04	Annika Asp, Henrika Littorin	Uppdatering av ordlista och konsekvensändring i texterna i enlighet med dokumentet HSA Begrepp och definitioner.
3.1.2	2021-06-28	Ronny Nilsson	Ändrat på formuleringen kring att ”Administrativa Uppdrag inte får användas för VoB"
3.2	2021-09-24	-	Godkänd av HSA Policygrupp
3.2.1	2022-04-30	Anders Malmros	Förtydligande av organisationsomfång för administrativa medarbetaruppdrag, kap 3.2.

1 Inledning

1.1 Syfte

Detta dokument beskriver den nationella behörighetsmodell som hanterar behörigheter inom vård och omsorg, både behörigheter som styrs direkt av patientdatalagen [1] (vårdmedarbetaruppdrag) och behörigheter som kan vara styrda av andra regelverk (administrativa medarbetaruppdrag).

Behörighetsmodellen utgår från arbetet inom AL-S (Arkitekturledningen – Säkerhet) med begrepps- och informationsmodeller för behörighetstilldelning enligt patientdatalagen [1], PDLiP [2], och har sedan utvecklats till en gemensam modell för att beskriva och tolka behörigheter. Modellen är implementerad i Katalogtjänst HSA och ligger till grund för behörighetshanteringen i ett stort antal nationella tjänster inom vård och omsorg. Förhoppningen är att den också ska användas i lokala och regionala utvecklingsprojekt samt av leverantörer till vård och omsorg.

1.2 Målgrupp

Följande målgrupper finns för detta dokument:

- De som beslutar om behörigheter (verksamhetschefer eller motsvarande)
- De som administrerar behörigheter
- Arkitekter och systemutvecklare
- Tjänster som hanterar behörigheter i sina system

1.3 Definitioner

Term	***Definition***
administrativt medarbetaruppdrag	*medarbetaruppdrag som används för att styra behörigheter som har administrativ karaktär och som inte omfattas av patientdatalagen, PDL [se mer i ref. 6]*
behörighetsområde	*(inom nationella behörighetsmodellen:) område som styrs av ett gemensamt regelverk för behörighetsstyrning [se mer i ref. 6]*
behörighetsområdesegenskap	*egenskap i ett medarbetaruppdrag som anger vilken behörighet en person har att få tillgång till viss information, utföra en viss aktivitet, inneha en viss roll eller kopplas till ett visst inloggningsförfarande inom ett behörighetsområde [se mer i ref. 6]*
medarbetaruppdrag	*uppdrag som tilldelas en medarbetare inom ett behörighetsområde som anger i vilken utsträckning och inom vilken giltighetstid denne har behörighet att hantera information inom ett visst organisationsomfång* *Medarbetaruppdrag består av olika kombinationer av egenskaper (s.k. behörighetsområdesegenskaper), vilka styr vilken typ av behörighet inom området som tilldelas.* Det finns idag två typer av medarbetaruppdrag: administrativt medarbetaruppdrag och vårdmedarbetaruppdrag, som används inom olika behörighetsområden. *[se mer i ref. 6]*
regelverksansvarig	*(inom nationella behörighetsmodellen:) person som ansvarar för det regelverk för behörighetsstyrning som ett behörighetsområde omfattas av när regelverket inte är lagstyrt [se mer i ref. 6]*
ansvarig för medarbetaruppdrag	*person som ansvarar för beslut om tilldelning och borttag av medarbetaruppdrag [se mer i ref. 6]*
vårdmedarbetaruppdrag	*medarbetaruppdrag som används för att styra behörighet av hälso- och sjukvårdskaraktär och som omfattas av patientdatalagen, PDL [se mer i ref. 6]*

2 Grunder och förutsättningar

Modellen är baserad på ett antal grundläggande förutsättningar främst baserade på lagar men också på praxis:

- **Personalen ska komma åt den information som de behöver för att utföra sitt arbete**
  - Det betyder att organisatoriska gränser inte ska sätta hinder om grundläggande krav inom behörighetsområdet är uppfyllda, t.ex. avtal, samtycke och vårdrelation
  - Behörigheter i IT-system är inte något som är frikopplat från personens uppdrag i verksamheten, utan ska harmoniera med dessa
- **Det är skillnad på behörighet och åtkomst**
  - Bara för att man har teknisk möjlighet (åtkomst) att titta på en uppgift betyder inte detta automatiskt att man är behörig att ta del av uppgiften[1]
  - Uppföljning av vem som gjort vad och varför är viktig
- **Behörigheten styrs av användarens och informationens egenskaper**
  - Behörigheter administreras inte i alla system utan kan hanteras i en egenskapskälla (till exempel HSA), detta eftersom behörigheten inte behöver vara system- eller applikationsberoende
  - Medarbetaruppdraget kan definiera det organisatoriska omfånget
- **Aktuella referensarkitekturer ska användas**
  - All implementation av behörighetsmodellen ska följa aktuella referensarkitekturer

[1] Ordet ”behörighet” definieras i informationssäkerhetsstandarden [3] som ’rättighet för en användare att använda informationstillgångar på ett specificerat sätt’. Ibland ser man att ordet ”åtkomst” också används med betydelsen ’*rättighet* att nå information’, men för undvikande av missförstånd bör ”åtkomst” endast avse ’*möjligheten* att nå information’. I standarden rekommenderas således denna betydelse av ”åtkomst”: ’interaktion mellan en användare och en resurs som resulterar i överföring av information dem emellan eller utnyttjande av resurser’.

3 Juridiska aspekter och regelverk

3.1 Juridiska aspekter för vårdmedarbetaruppdrag

De juridiska aspekterna av behörighetsstyrning för vårdmedarbetaruppdrag inom hälso- och sjukvård styrs av patientdatalagen (PDL) [1] som innehåller en samlad reglering av IT-relaterad informationshantering inom hälso- och sjukvården. Syftet med lagen är att hanteringen av personuppgifter inom hälso- och sjukvården ska underlättas samtidigt som patientsäkerheten och patientens egen möjlighet till medverkan ska stärkas. Lagen är utformad för att underlätta informationsutbyte mellan vårdgivare [4] och mellan vårdgivare och patient, med skyddet för patientens integritet som hög prioritet. Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården (HSLF-FS 2016:40 [5]) kompletterar PDL med mer konkreta anvisningar.

HSLF-FS 2016:40 tydliggör att det är vårdgivaren som ansvarar för att ta fram och dokumentera rutiner så att personalens behörigheter begränsas till vad som är nödvändigt för att ge en god och säker vård. Behörighetstilldelningen ska föregås av en behovs- och riskanalys. Behörigheter för åtkomst till patientuppgifter ska vara individuella och anpassade för att en och samma individ kan ha flera olika arbetsuppgifter vid olika tidpunkter. Detta innebär att behörighetssystemen måste ta hänsyn till olika uppdrag och olika ändamål med åtkomst till patientuppgifter. Vårdgivaren ska även ansvara för att det finns rutiner för regelbunden uppföljning av behörigheterna.

Vårdgivaren ansvarar för att individuell behörighetstilldelning sker så att utdelade behörigheter för åtkomst till patientuppgifter är ändamålsenliga och förenliga med hälso- och sjukvårdspersonalens och andra befattningshavares aktuella arbetsuppgifter. Behörighetsmodellen bygger i nuläget på att vårdgivaren utser verksamhetschefen som ansvarig för medarbetaruppdrag.

Behörighetstilldelningen avser såväl åtkomst inom den egna vårdenheten, som andra vårdenheter hos den egna vårdgivaren samt direktåtkomst till annan vårdgivare som deltar i system för sammanhållen journalföring.

Vid behovsbedömning och behörighetstilldelning ska man skilja på aktiviteterna läsa[2], skriva[3], signera[4] och utskrift[5]. Vid den egna vårdenheten är alla aktiviteterna möjliga medan utanför den egna vårdenheten endast läsning är tillåten.

2 Läsa = Ta del av information utan att påverka den.

3 Skriva = Skapa information, lägga till information till redan befintlig samt ändring av icke låst information. Omfattar inte radering/makulering av låst information och inte heller ingår signering i någon form.

4 Signera = påföra signatur i syfte att styrka riktighet och säkerställa spårbarhet.

5 Utskrift = kopiera information till papper via direkt utskrift. Här ingår inte kopiering av information till andra media.

Läsning av patientinformation utanför den egna vårdgivaren – alltså med omfånget sammanhållen journalföring (SJF) – är endast tillåten med ändamålet Vård och behandling (jämför [1], 6 kap. 3 §).

Administrationen av behörigheter bör vara utformad så att både vårdgivare och den som tilldelats behörighet har tillgång till information som på ett tydligt sätt visar vilka behörigheter som tilldelats och vilka uppdrag som därmed skall fullgöras.

Denna behörighetsmodell är endast avsedd att användas för elektronisk åtkomst/direktåtkomst till patientinformation.

3.2 Regelverk för administrativa medarbetaruppdrag

När det gäller administrativa medarbetaruppdrag finns, till skillnad från när det gäller vårdmedarbetaruppdrag, ingen gemensam lagstiftning som beskriver t.ex. ändamål eller behörighetsegenskaper. Däremot kan ett enskilt behörighetsområde lyda under specifik lagstiftning. Varje behörighetsområde måste definiera sitt eget behörighetsregelverk som beskriver vilka behörighetsområdesegenskaper som finns och hur de får användas. Regelverken ska vara dokumenterade och publicerade.

Organisationsomfång för det administrativa medarbetaruppdraget avgörs i normalfallet av dess placering i organisationsstrukturen (exempelvis HSA) och gäller där medarbetaruppdraget är placerat och nedåt i hierarkin.

Möjlighet finns dock både

- att välja annan enhet,
- att reglera organisationsomfånget till enskild enhet eller inkludera dess underliggande enheter,
- samt att välja "organisationslöst" för behörighetsområdesegenskaper där koppling till organisation inte är relevant

Regelverksansvarig ansvarar för behörighetsstyrningen och anges i uppdraget.

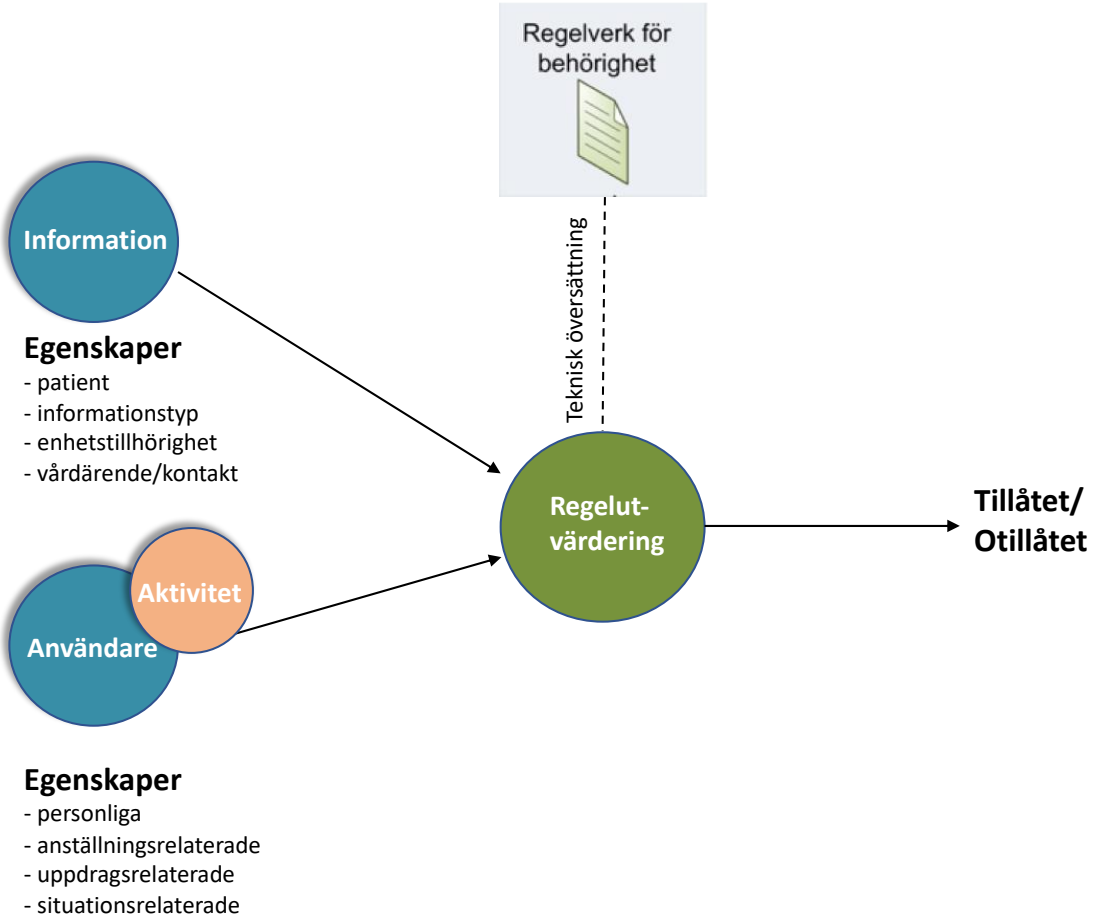
Den juridiska personen, organisationen, utgör gränsen för hur omfattande ett administrativt medarbetaruppdrag kan göras. Anledningen till detta är att det inte går att fastställa ansvarig person utanför den egna organisationen. Om en person ska tilldelas en behörighet som omfattar flera juridiska personer så går det att hantera, se bilaga 2 ”Administrativa medarbetaruppdrag”.

4 Egenskapsbaserad behörighet

Traditionellt administreras användare i varje system för sig. Konsekvensen i en decentraliserad organisation som vård och omsorg, med många system, är stor administration av användare, att användare har olika identiteter och lösenord i alla olika system och att det är svårt, för att inte säga omöjligt, att få en totalbild av en användares behörigheter.

Egenskapsbaserad behörighet ger förutsättningar för systemoberoende behörighetshantering med höga krav på riktighet och spårbarhet där informationen om vilka behörigheter en användare har finns samlad på ett ställe.

Egenskapsbaserad behörighet innebär att behörigheter ges utifrån att gemensamt definierade egenskaper, som användaren och informationen innehar, processas i ett gemensamt regelverk. Resultatet kan användas i alla system som hanterar information och användare inom de områden för vilka modellen finns definierad. Egenskaperna i sig ger inga behörigheter. Användarens egenskaper måste först matchas med egenskaper hos den information användaren önskar åtkomst till. ***Det är när användaregenskaperna värderas mot informationsegenskaper enligt regelverket som behörigheterna utvärderas.*** En sådan utvärdering sker i någon form av regelmotor i respektive tjänst.



Figur 1 Informationens och användarens egenskaper kontrolleras i regelutvärderingen.

För vårdmedarbetaruppdrag är det den av vårdgivaren utsedda verksamhetschefen (uppdragsansvarig person) som beslutar vilken informationsmängd en användare med uppdrag åt verksamheten ska få tillgång till, inte den enhet som har producerat informationen eller den som förvaltar systemet. Behörighet regleras även genom överenskommelse om sammanhållen journalföring, vårdrelation, samtycke och spärr.

4.1 Användaregenskaper

4.1.1 Personliga egenskaper

Personliga egenskaper är egenskaper som användaren har oavsett om hen är ledig eller arbetar, är anställd eller arbetslös. Dessa egenskaper har lång varaktighet, i de flesta fall har användaren dem hela livet när de väl förvärvats.

Dessa egenskaper lagras i attributkällan och de flesta av dem hämtas från och/eller kontrolleras mot externa källor som befolkningsregistret eller Socialstyrelsens register över legitimerad hälso- och sjukvårdspersonal, HOSP.

Exempel på sådana egenskaper är personnummer, yrkeslegitimation och personlig förskrivarkod.

4.1.2 Anställningsrelaterade egenskaper

Anställningsrelaterade egenskaper erhåller användaren i samband med anställningen. Användaren har dem så länge som hen innehar en viss tjänst hos en viss arbetsgivare vilket innebär att varaktigheten kan vara allt från många år till dagar. Dessa egenskaper lagras i attributkällan och hämtas från/kontrolleras mot personalsystem eller liknande.

Exempel på sådana egenskaper är befattningskod.

4.1.3 Uppdragsrelaterade egenskaper

Egenskaper relaterade till medarbetaruppdrag erhåller användaren när hen har ett aktivt uppdrag. Administrativa medarbetaruppdrag som en användare är kopplad till ses alltid som aktiva. För vårdmedarbetaruppdrag räcker det inte med att användaren är kopplad till ett uppdrag, användaren måste också ha valt att använda just det uppdraget. Personen kan bara ha ett vårdmedarbetaruppdrag i taget aktivt. Varaktigheten på dessa egenskaper blir alltså till användaren byter vårdmedarbetaruppdrag eller loggar ut.

Exempel på uppdragsrelaterade egenskaper för ett vårdmedarbetaruppdrag är ändamål för åtkomst till patientdata och koppling till vårdenhet. Exempel på uppdragsrelaterade egenskaper för administrativa medarbetaruppdrag är behörighetsområdesegenskap.

4.1.4 Situationsrelaterade egenskaper

Situationsrelaterade egenskaper uppstår under användandet. Några exempel på situationsrelaterade egenskaper är patientrelation, samtycke, tid på dygnet och autentiseringsmetod.

Dessa egenskaper hämtas inte från någon beständig attributkälla utan de uppstår under användandet och finns normalt bara kvar, som längst, under aktuell session. Ett undantag är samtycke som kan gälla under ett specificerat tidsintervall.

4.2 Informationsegenskaper

Informationens egenskaper kan delas in i tidsbundna (till exempel skapandetidpunkt), ägarskap (till exempel vårdenhet eller organisation) och innehåll (till exempel informationstyp). Egenskaperna har inte samma skillnader på varaktighet som egenskaper på användaren. Egenskaperna tillkommer vid skapandet och kan bara ändras om informationen ändras då de är en integrerad del av informationen.

En konsekvens av detta är att det är svårt att lägga på egenskaperna på informationen i efterhand. Informationen skapas dessutom ofta i system med mycket långa förändringscykler. Det är därför mycket viktigt att regelverket för vilka egenskaper som krävs på informationen inte ändras ofta och att man inser att eventuella ändringar kan ta flera år att bli realiserade och då oftast inte kan appliceras på information som skapats tidigare.

4.3 Regelutvärdering

Som redan beskrivits är nyckeln till behörigheten det regelverk där användaregenskaperna matchas mot informationsegenskaperna eller behörighetsområdesegenskaperna. Det är viktigt att regelverket i grunden är formulerad i en form som kan läsas och tolkas utan expertkunskaper. Metoder måste finnas för att kvalitetssäkra översättningen till regelutvärderingens tekniska format.

5 Förvaltning av behörighetsmodellen

Förvaltning i detta sammanhang betyder såväl daglig hantering av användardokumentation, support och stöd till vårdgivare och tjänsteförvaltare avseende tillämpning av modellen som långsiktigt arbete med att hålla modellen aktuell.

Behörighetsmodellen består av begreppsmodell och informationsmodell från PDLiP [2] samt regelverk. Dessa behöver uppdateras allteftersom tillämpning och erfarenheter utvecklas. Anpassningar behöver också göras om lagar och förordningar ändras.

Arbetet med beredning av ändringsförslag sker inom ramen för befintlig förvaltningsstruktur (HSA Förvaltning) men med god tillgång till kompetens inom juridik, teknik, informatik och verksamhet (Arkitektur och Regelverk på Inera). För detta arbete krävs förankring och legitimitet hos berörda parter så att resultatet inte ifrågasätts.

6 Råd vid användning av behörighetsmodellen

Användning av behörighetsmodellen betyder att de enskilda användarna (individerna) inte ska administreras i ett lokalt behörighetskontrollsystem i den egna applikationen utan egenskaper hämtas från en egenskapskälla (= nationell eller lokal katalogtjänst). Egenskapskällan administreras inom användarorganisationen och inte av system-/informationsägaren. Det informations-/systemägaren gör är att formulera ett regelverk för åtkomst till informationen.

Det innebär att det första som behöver definieras är vilka typer av användare som skall ha åtkomst till informationen i det egna systemet

- För vårdmedarbetaruppdrag: Personal inom egna vårdenheten (inre sekretess), inom vårdgivaren eller alla i vården
- Är det bara någon speciell yrkeskategori som får skriva? Läkare, sjuksköterskor, annan legitimerad personal, befattning eller bara speciellt certifierad och utbildad personal?
- Finns det någon uppdelning på olika informationstyper och behöver behörigheter särskiljas med avseende på detta?
- Finns det några undantag eller avvikelser när det gäller vilka som får behörigheter i systemet?

Efter denna analys behöver en genomgång göras av vad det är som kännetecknar de typer av användare man identifierat. Exempelvis kan legitimation, befattning eller specialistutbildning användas. Kan man använda redan befintliga egenskaper i egenskapskällan är det en fördel. Varje egenskap som inte behöver administreras manuellt är en felkälla/arbetsuppgift mindre!

Detta behöver sedan dokumenteras i ett regelverk som går att tekniskt implementera i en regelmotor.

Sedan krävs naturligtvis en tydlig dokumentation riktad till användare och administratörer om vad som gäller, och i många fall även en välplanerad informationsinsats.

Refererade dokument

Ref. nr	Namn	Länk till publicerad version
[1]	Patientdatalag (2008:355)	https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/patientdatalag-2008355_sfs-2008-355
[2]	PDLiP RIV ver 1.0	Dokumentet finns inte längre publicerat då det sedan införandet av Socialstyrelsens nya föreskrifter HSLF-FS 2016:40 inte längre är giltigt i alla delar.
[3]	SIS-TR 50:2015 Terminologi för informationssäkerhet	https://www.sis.se/
[4]	Förtydliganden Vårdgivare Vårdenhet	https://inera.se/hsa/dokument under rubriken Stödjande
[5]	HSLF-FS 2016:40	http://www.socialstyrelsen.se
[6]	HSA Begrepp och definitioner	https://inera.se/hsa/dokument under rubriken Stödjande

Bilaga 1 Vårdmedarbetaruppdrag

Inledning

Bakgrund

Detta är en bilaga till Behörighetsmodell för vård och omsorg och beskriver hur vårdmedarbetaruppdrag är uppbyggda och fungerar. Vårdmedarbetaruppdrag används för att styra åtkomst till information och funktioner som är patientinformationsrelaterade, det vill säga lyder under patientdatalagen, PDL [1].

1.1. Vårdmedarbetaruppdrag är systemoberoende

En bärande idé för vårdmedarbetaruppdrag i den nationella behörighetsmodellen är att de ska vara systemoberoende, det vill säga att det inte ska spela någon roll i vilket system/vilken tjänst informationen hanteras. Har användaren behörighet till informationen ska användaren ha tillgång till den oavsett teknisk lösning. Detta är en grundläggande egenskap för vårdmedarbetaruppdrag.

Kravet på systemoberoende behörigheter leder till en behörighetsutvärdering där det genereras en ”behörighetsfråga” per kombination användare, aktivitet och informationsmängd. För varje fråga ska regelutvärderingen svara om det är tillåtet eller otillåtet med åtkomst.

1.2. Egenskaper hos ett vårdmedarbetaruppdrag

Egenskaperna hos ett vårdmedarbetaruppdrag baseras på de begrepps- och informationsmodeller som togs fram i projektet Patientdatalagen i praktiken [2] som genomfördes 2008–2009 och uppdaterades 2011. I den analysen framkom att för att behörigheten ska kunna avgöras måste vårdmedarbetaruppdraget upplysa om:

- Vilken vårdgivare som användaren är knuten till (obligatorisk egenskap)
- Vilken vårdenhet som användaren är knuten till (obligatorisk egenskap vid ändamålet Vård och behandling)
    - I dagens tekniska implementation är även vårdenhet en obligatorisk egenskap i alla sammanhang, inte bara i samband med ändamålet Vård och behandling.
- Vilket ändamål användaren har med informationshanteringen (obligatorisk egenskap)
    - De befintliga ändamålen är givna av patientdatalagen [1]
- Vilken eller vilka typer av aktiviteter användaren har behörighet att utföra
    - Eftersom efterfrågan varit sparsam och förvaltningen obefintlig finns för närvarande endast en aktivitet bland de aktiva koderna. Den aktiviteten är *läsa*.

- Vilken eller vilka typer av information som användaren har behörighet att hantera
    - Eftersom efterfrågan varit sparsam och förvaltningen obefintlig finns för närvarande endast en rudimentär lista av informationstyper endast anpassade för Nationell Patientöversikt, NPÖ.
- Vilket eller vilka organisationsomfång som användaren har behörighet inom
    - De tre nivåerna som finns är inom användarens *vårdenhet*, inom användarens *vårdgivare* eller inom den *sammanhållna journalföringen (SJF)*. Det är även möjligt att ange omfång till en lägre nivå än vårdenhet (en enskild enhet som ingår i en vårdenhet, till exempel en mottagning eller avdelning) – dock inte i kombination med aktiviteten *läsa*.

1.3. Utmaningar och möjligheter med modellen

De olika delarna som tillsammans bygger ett vårdmedarbetaruppdrag har hittills inte utnyttjats i sin fulla potential. Det finns inte något uppdrag att aktivt förvalta de olika kodverken för egenskaperna som styr vilken åtkomst som ska göras möjlig via ett uppdrag. Informationstyperna togs fram inför starten av NPÖ, men har aldrig använts annat än som "alla".

Det finns utvecklingspotential i behörighetsmodellen genom att utveckla och differentiera användandet av informationstyper. Genom att mer aktivt styra olika vårdmedarbetaruppdrag på vilken informationstyp det aktuella uppdraget omfattar, finns en stor möjlighet att rikta rätt behörighet till rätt informationstyp. Det ger också möjligheten att koppla mer differentierad behörighet till själva vårdmedarbetaruppdraget och inte lägga det som egna attribut kopplat till enskild person.

2. Praktisk användning av modellen

2.1. Exempel på vårdmedarbetaruppdrag

Personal markerar sin tillhörighet till enheten genom att bli tilldelad ett vårdmedarbetaruppdrag. Personal som har vårdmedarbetaruppdrag på flera vårdenheter måste välja vilket som är aktuellt för tillfället.

2.1.1. Vårdmedarbetaruppdrag Normalläget

De flesta vårdmedarbetaruppdrag har följande egenskaper.

Namn (förslag)	Ändamål	Aktivitet	Informationstyp	Omfång
VoB <vårdenhetsnamn>	Vård och behandling	läsa	alla[6]	SJF[7]

Detta uppdrag ger tillgång till flera nationella tjänster bland annat Pascal och NPÖ.

2.1.2. Vårdmedarbetaruppdrag Spärr och logg

Vårdmedarbetaruppdrag för spärr och logghantering har följande egenskaper.

Namn (förslag)	Ändamål	Aktivitet	Informationstyp	Omfång
Spärr och logg <vårdenhetsnamn>	Administration	-	-	-

Detta uppdrag ger bland annat tillgång till hantering av spärr och logg i säkerhetstjänsterna.

I säkerhetstjänsterna tolkas uppdraget oavsett vilken vårdenhet som pekas ut som gällande för hela vårdgivaren. Här skulle det vara önskvärt att möjligheten fanns att ha vårdmedarbetaruppdrag på vårdgivarnivå, men detta är ännu inte realiserat.

2.1.3. Vårdmedarbetaruppdrag kvalitetssäkring

Vårdmedarbetaruppdrag för kvalitetssäkring har följande egenskaper.

Namn (förslag)	Ändamål	Aktivitet	Informationstyp	Omfång
Kvalitetssäkring <vårdenhetsnamn>	Kvalitetssäkring	läsa	alla	VE

Detta uppdrag ger till exempel behörighet för registerutdrag och koppling av postoperativa infektioner till utförda åtgärder i tjänsten Infektionsverktyget.

[6] I och med att informationstypen ”alla” används innebär det automatisk åtkomst till eventuella framtida informationstyper. Detta beaktas i förvaltningen av kodverket Medarbetaruppdragets rättigheter informationstyp.

[7] SJF är koden för sammanhållen journalföring.

2.2. Teoretiskt exempel på användning

I detta avsnitt beskrivs ett teoretiskt exempel på hur vårdmedarbetaruppdrag skulle kunna utvecklas.

I exemplet nedan har ett vårdmedarbetaruppdrag skapats som skulle kunna ge den som fått det tilldelat rätten att signera att man har lämnat ut ett läkemedel.

Namn (förslag)	Ändamål	Aktivitet	Informationstyp	Omfång
VoB <vårdenhetsnamn>	Vård och behandling	Signera	lkm	VE

I exemplet har vi använt delar av kodverket som normalt inte används idag. Dels en aktivitet, *signera*, och dels en specifik informationstyp, *lkm*.

Det finns några aktiviteter, förutom *läsa*, som är definierade men inte tillförda i kodverket, se nedan:

Aktivitet	Definition
Skriva	*”Skapa information, lägga till information till redan befintlig samt ändring av icke låst information. Omfattar inte radering/makulering av låst information och inte heller ingår signering i någon form.”*
Signera	*” Påföra signatur i syfte att styrka riktighet och säkerställa spårbarhet”*
Utskrift	*"Kopiera information till papper via direkt utskrift. Här ingår inte kopiering av information till andra media"*

För informationstyp har vi använt *lkm*, vilket betyder ”läkemedel utlämning”.

För omfång har vi valt VE (vårdenhet). Värt att notera är att så fort man har en annan aktivitet än läsa så är organisationsomfånget SJF *inte* tillåtet.

Bilaga 2 Administrativa medarbetaruppdrag

1. Bakgrund

Detta är en bilaga till den nationella behörighetsmodellen och beskriver hur administrativa medarbetaruppdrag är uppbyggda och fungerar. Administrativa medarbetaruppdrag används för att styra åtkomst till information och funktioner som kan vara styrda av andra regelverk. Exempelvis olika redaktionella uppdrag inom 1177 och personaladministration.

Administrativa medarbetaruppdrag skiljer sig från vårdmedarbetaruppdrag på följande vis:

- behörigheter behöver kunna ges för andra enheter än vårdenheter
- variationen i lagrum, informationsmängder, ändamål och organisationsomfång är mycket stor
- det är olika chefer som tilldelar rättigheter till olika informationsmängder för samma enhet/organisation

Ett exempel på användning är som komplement till vårdmedarbetaruppdrag för att specificera en eller flera egenskaper för en person vid inloggning i vårdsystem där fler uppdragsrelaterade egenskaper behöver vara definierade för att personen ska kunna tilldelas rätt behörighet.

Ett mål med skapandet av administrativa medarbetaruppdrag är också att komma ifrån, eller åtminstone kraftigt minska, användningen av systemroller på personer (*hsaSystemRole*). Denna användning ger svåröverskådliga behörigheter som är svåra att administrera korrekt över tid och som saknar möjlighet att begränsa organisationsomfånget.

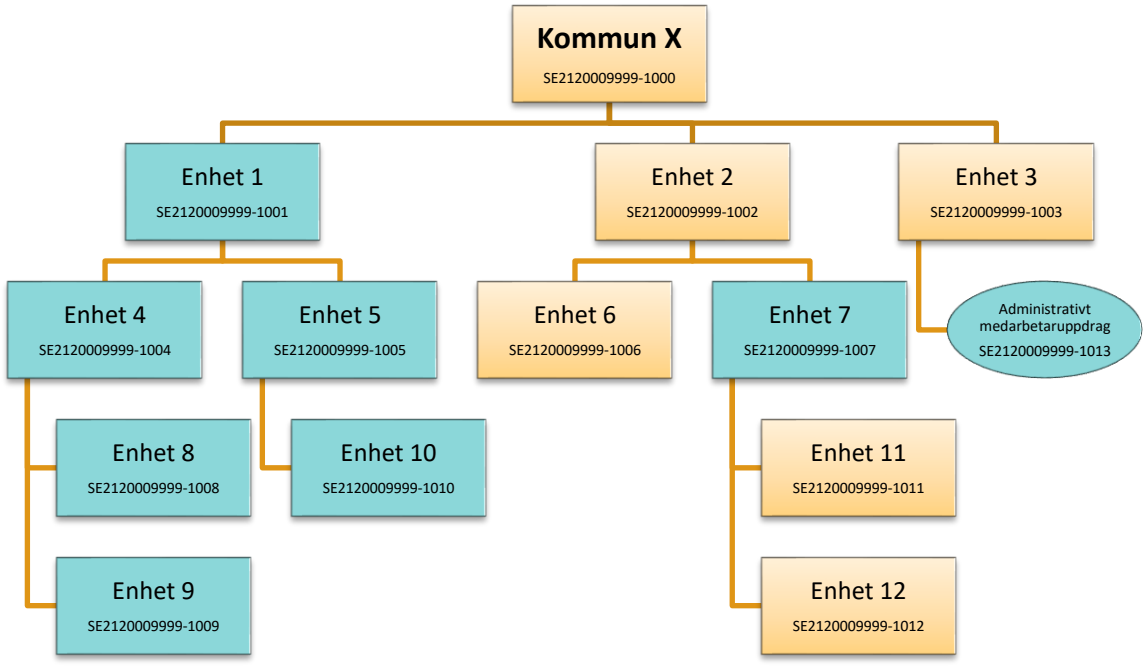
Administrativa medarbetaruppdrag har följande utgångspunkter:

- **Hanteringen av administrativa medarbetaruppdrag liknar vårdmedarbetaruppdrag**
  Det förenklar för katalogadministratörerna och möjliggör återanvändning av redan framtagna gränssnitt på nationell och lokal nivå.
- **Organisatoriskt omfång kan beskrivas i uppdraget**
  Det organisatoriska omfånget kan sättas att gälla från den startpunkt (=enhet) som anges i uppdraget och nedåt i organisationshierarkin.[8] Men möjlighet finns också att i uppdraget ange exakt de enheters HSA-id:n som uppdraget ska gälla för (se figur 1). Ett

[8] Ska bara användas om uppdraget ska gälla för hela den underliggande organisationshierarkin.

administrativt medarbetaruppdrag kan bara gälla inom den egna organisationen (inom HSA; det egna o:et).

- **Ansvarig ska anges i uppdraget**
  I och med att den tydliga kopplingen till ansvarsområde, som finns i fallet ”Vårdenhet”, saknas för administrativa medarbetaruppdrag ska ansvarig för medarbetaruppdraget anges direkt i det administrativa medarbetaruppdraget.
- **Uppdrag kan kopplas till uppdrag**
  Ett kraftfullt sätt att hantera distribuerad administration är att använda andra uppdrag som ”listor” på personer. Genom att koppla ett annat uppdrag som ett ”underuppdrag” kan medlemmarna i underuppdraget ges huvuduppdragets rättigheter. De uppdrag som ska kopplas kan vara placerade var som helst inom attributkällan.
- **Egenskaperna för administrativa medarbetaruppdrag styrs utifrån respektive behörighetsområde**
  För administrativa medarbetaruppdrag styrs vilka egenskaper som ska finnas från den/de behörighetsområden (se nedan) som uppdraget ska gälla för.
- **Alla administrativa medarbetaruppdrag är aktiva samtidigt**
  Det betyder alltså att användaren aldrig behöver välja några administrativa medarbetaruppdrag.



Figur 2 Administrativt medarbetaruppdrag som pekar ut uppdragets organisatoriska omfång genom att peka ut ett helt delträd samt genom att ange en unik enhet.

2. Modellen

Det är inte bara system som kan ha krav på en anpassad, unik behörighetsstruktur. Som ett generellt uttryck har ordet *behörighetsområde* valts för att beteckna det område inom vilket behörigheten gäller. Ett behörighetsområde kan alltså vara ett enskilt system men också en tjänst.

Konceptet med regelutvärdering bygger på en jämförelse mellan användarens egenskaper och egenskaperna i behörighetsområdet. På grund av variationsbredden hos olika behörighetsområden kan ingen generalitet i regelutvärderingen skapas utan den ägs helt av respektive behörighetsområde. Regelverksansvariga måste ta fram en beskrivning av vilka egenskaper som används i behörighetsområdets regelmotor och vilka kombinationer som ger vilken behörighet inom behörighetsområdet.

3. Behörighetsområden

I modellen delas behörighetsområden in i *behörighetsområdesegenskaper* för att hantera olika typer av rättigheter. Administrativa medarbetaruppdrag bygger på att administratören väljer bland behörighetsområdesegenskaperna för att ange den eller de som är lämpliga för att uppdraget ska ge rätt behörighet. Ett administrativt medarbetaruppdrag kan alltså innehålla flera behörighetsområdesegenskaper inom flera olika behörighetsområden, vilket gör att en grupp medarbetare på ett enkelt sätt kan tilldelas flera behörigheter som de behöver i sitt uppdrag.

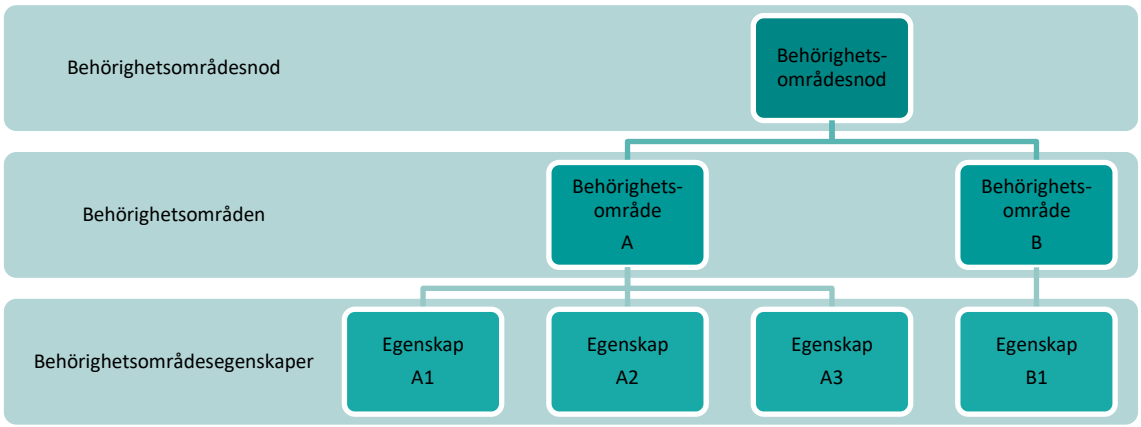
Ett behörighetsområde kan utgöras av ett enskilt system men också en tjänst eller ett större område inom vilket samma typ av behörighetsstyrning tillämpas. Varje behörighetsområde har sitt eget regelverk. Behörighetsområdets egenskaper styrs av det aktuella regelverket för behörighetsstyrning. På grund av olikheterna hos olika behörighetsområden kan ingen generalitet i regelutvärderingen skapas utan den ägs helt av respektive behörighetsområde.

Varje behörighetsområde har en ansvarig person, regelverksansvarig, som förvaltar behörighetsområdet och dess egenskaper. Regelverk och behörighetsstruktur för ett behörighetsområde måste vara helt klar innan registrering i HSA påbörjas.

Behörighetsområdet tillgängliggörs via de lokala administrationsgränssnitten och behörighetsområdesegenskaper kan inlemmas i ett administrativt medarbetaruppdrag.

Anslutande tjänster kan återanvända redan befintliga behörighetsområden och dess egenskaper. T.ex. skulle anslutna ekonomisystem kunna ha ett gemensamt behörighetsområde som ger liknande behörigheter i varje ekonomisystem. Detta skulle minska administrationsbördan för regelverksansvarig.

I bilden nedan visas hur behörighetsområden byggs upp genom behörighetsområdesobjekt och behörighetsområdesegenskapsobjekt.



Figur 3 Schematisk bild över uppbyggnaden av behörighetsområde.

3.1 Struktur för behörighetsområden

Följande gäller för lagring och registrering av behörighetsområden:

- Varje behörighetsområde har en gren i behörighetsområdesträdet (dc=AuthorizationAreas) där behörighetsområdesspecifika egenskaper lagras.
- Varje behörighetsområde ska ha en utpekad regelverksansvarig.

Ett behörighetsområde ska ha följande attribut, dessa lagras i ett ***behörighetsområdesobjekt (objectClass=hsaDomain)***:

Attribut	Attributets LDAP-namn[9]	Beskrivning	Kommentar
namn	*cn*	Hämtas till förvalslistan för behörighetsområden som visas för administratören.	Unikt Obligatoriskt
HSA-id	*hsaIdentity*		Unik Obligatoriskt
behörighetsområdeskod	*hsaDomainCode*	Ett unikt prefix som ska inleda alla koder inom behörighetsområdet för att göra dem globalt unika. Prefix som ska vara tillgängliga nationellt tilldelas genom HSA Förvaltning.	Unik Obligatorisk
beskrivning	*description*	Behörighetsområdets fullständiga namn, kort beskrivning av vilka personer som kan vara aktuella för rättigheter samt kontaktuppgifter för önskemål om förändringar i värdemängder. Texten är till stöd för en administratör som ska välja rätt behörighetsområde vid administration av uppdrag. Ska kunna visas i administrationsgränssnitten.	Obligatorisk
Regelverksansvarig	*hsaDomainResponsible*	Information om ansvarig organisation och person samt dennes roll/funktion, t.ex. tjänsteansvarig eller förvaltare.	Obligatorisk, fritext

3.2 Struktur för behörighetsområdesegenskaper

Under behörighetsområdet skapas ***behörighetsområdesegenskaper (objectClass=hsaDomainArea)***, som innehåller följande attribut:

[9] Denna kolumn visar LDAP-namnen på attributen som används i HSA.

Attribut	Attributets LDAP-namn[10]	Beskrivning	Kommentar
namn	*cn*	Hämtas till förvalslistan för behörighetsområdesegenskaper som visas för administratören.	Unikt inom behörighetsområdet Obligatoriskt
HSA-id	*hsaIdentity*		Obligatoriskt
kod för behörighetsområdesegenskap	*hsaDomainAreaCode*	Den kod som behörighetsområdets regelmotor ska känna igen och utvärdera.	Obligatorisk Unik kod, inleds med behörighetsområdeskoden
beskrivning	*description*	Kort beskrivning av behörighetsområdesegenskapen. Huvudsyftet är att hjälpa administratören att välja rätt behörighetsområdesegenskap vid administration av uppdrag.	Obligatorisk
begränsning av behörighets-områdesegenskap	*hsaDomainAreaAllowed*	En möjlighet för regelverksansvarig att begränsa organisationer/enheter som får använda behörighetsområdet i administrativa uppdrag. Begränsningen anges med HSA-id för den eller de organisationer/enheter som får använda behörighetsområdet. Om inget HSA-id anges kan behörighetsområdet knytas till alla organisationer/enheter.	Frivilligt Flervärt Kan bara innehålla HSA-id;sub.

3.3 Förvaltning av behörighetsområden

Varje behörighetsområde är unikt, och det är inte alltid möjligt att hämta regelverket från befintlig dokumentation. Varje regelverksansvarig måste därför leverera en beskrivning av behörighetsområdets behörighetsmodell enligt en mall utformad av HSA Förvaltning.

[10] Se referens 2.

Behörighetsområdet skapas i HSA av HSA Förvaltning som lägger till information om regelverksansvarig och tilldelar behörigheter att administrera behörighetsområdet till denne. Endast tjänster som använder HSA som källa för behörigheter och har någon form av överenskommelse med HSA Förvaltning kan få ett behörighetsområde i behörighetsområdesträdet.

Därefter skapar regelverksansvarig underliggande behörighetsområdesegenskaper.

Regelverksansvarig för behörighetsområdet måste ha en plan för hur man tar emot och behandlar önskemål om förändringar, hur beslut om förändringar fattas, vem som kan ta beslut om förändringar samt hur förändringar kommuniceras till berörda. Varje regelverksansvarig har ansvar för att förmedla sin behörighetsmodell till användarna. Möjlighet finns dock att ”köpa” den praktiska administrationen av behörighetsområdet.

Behörighetsområden som ej längre ska användas raderas av HSA Förvaltning. Regelverksansvarig ansvarar för eventuellt behov av arkivering.

4. Administrativa medarbetaruppdrag

4.1 Struktur på administrativa medarbetaruppdrag

Följande gäller för lagring och registrering av administrativa medarbetaruppdrag:

- Administrativa medarbetaruppdrag får skapas under organisationer (objectClass=organization) samt under alla typer av enheter (objectClass=organizationalUnit), såvida inte något organisationsomfång för behörighetsområdesegenskap finns.

Administrativa medarbetaruppdrag (objectClass=hsaAdminCommission) kan innehålla följande information:

Attribut	**Attributets LDAP-namn[11]**	**Beskrivning**	**Kommentar**
namn	*cn*	Uppdragets namn.	Obligatoriskt
HSA-id	*hsaIdentity*		Obligatoriskt
beskrivning	*description*	Beskrivning av uppdraget.	Frivilligt

[11] Denna kolumn visar LDAP-namnen på attributen som används i HSA.

Attribut	Attributets LDAP-namn[11]	Beskrivning	Kommentar
uppdragsansvarig organisation, administrativa medarbetaruppdrag	*hsaAdminCommissionResponsibleOrganization*	HSA-id för den organisation som ansvarar för uppdraget. Organisation som pekas ut måste ha organisationsnummer angivet.	Frivilligt
uppdragsansvarig person, administrativa medarbetaruppdrag	*hsaAdminCommissionResponsiblePerson*	HSA-id för den person som ansvarar för uppdraget.	Frivilligt
administrativa medarbetaruppdragets behörighetsområdesegenskaper	*hsaDomainAreaCode*	De koder för behörighetsområdesegenskaper som kopplas till uppdraget.	Frivilligt Flervärt
administrativa medarbetaruppdragets medlemmar, personer	*hsaAdminCommissionMemberP*	HSA-id för de personer som har uppdraget samt eventuellt start- och slutdatum.	Frivilligt Flervärt
administrativa medarbetaruppdragets medlemmar, andra uppdrag	*hsaAdminCommissionMemberC*	HSA-id för ett annat administrativt medarbetaruppdrag vars medlemmar har detta uppdrag samt eventuellt start- och slutdatum.	Frivilligt Flervärt
administrativa medarbetaruppdragets organisationsomfång	*hsaAdminCommissionSector*	Uppdraget gäller för den/de enheter (HSA-id:n) som anges. Om en flagga anges för att enheten är en hierarkisk startpunkt så gäller uppdraget från denna enhet och nedåt. Det är respektive informationsägande organisation som avgör om man vill använda principen med flagga för hierarkisk startpunkt eller enbart tillåta att enskilda enheter pekas ut med hjälp av HSA-id.	Frivilligt Flervärt

4.1.1 Uppdrag som är medlem i ett uppdrag

Möjligheten att ange ett administrativt medarbetaruppdrag som medlem i ett annat administrativt medarbetaruppdrag används i de fall då en uppdragsadministratör vill ge rättigheter till en grupp inom ett annat område men inte själv vill administrera gruppens medlemmar.

Regelverket ser ut så här:

- *Huvuduppdrag*: Ett uppdrag som innehåller behörighetsområdesegenskaperna (rättigheterna)
- *Underuppdrag:* Ett uppdrag som kopplas som medlem till Huvuduppdraget, används i det här sammanhanget bara som lista på personer. Underuppdraget kan ha egna behörighetsområdesegenskaper men dessa har ingen betydelse i detta sammanhang.
- Administratören för Huvuduppdraget är den som kan koppla ihop och koppla isär uppdragen. Ihopkopplingen förutsätter att det finns en överenskommelse mellan ansvarig för *Huvuduppdraget* och *Underuppdraget* men ansvaret för *Huvuduppdraget* gentemot regelverksansvarig förblir oförändrat.
- Kopplingen gäller bara en nivå.

I exemplet nedan är det administrativa *medarbetaruppdraget B* medlem i *medarbetaruppdrag A*. *medarbetaruppdrag C* är i sin tur medlem i *medarbetaruppdrag B*. Men medlemmarna i *medarbetaruppdrag C* får inte behörighetsområdesegenskaperna från *medarbetaruppdrag A*.

Administrativt medarbetaruppdrag A

Personmedlem:
- Olle
- Börje

Gruppmedlem
- Uppdrag B

Behörighetsområdesegenskap
- BOE1;001
- BOE2;002

Administrativt medarbetaruppdrag B

Personmedlem:
- Frans
- Hjördis

Gruppmedlem
- Uppdrag C

Behörighetsområdesegenskap
- BOE1;002

Administrativt medarbetaruppdrag C

Personmedlem:
- Arvid
- Eva

Gruppmedlem
-

Behörighetsområdesegenskap
- BOE2;001

Resultat behörigheter

Person	har	Behörighetsområdesegenskaper		
Olle		BOE1;001	BOE2;002	
Börje		BOE1;001	BOE2;002	
Frans		BOE1;002	BOE1;001	BOE2;002
Hjördis		BOE1;002	BOE1;001	BOE2;002
Arvid		BOE2;001	BOE1;002	
Eva		BOE2;001	BOE1;002	

Figur 4 Exempel på administrativt medarbetaruppdrag som innehåller medlemmar från andra administrativa medarbetaruppdrag.

Notera att uppdrag som är medlemmar i uppdrag inte används idag och därmed inte heller kan hanteras i befintligt administrationsgränssnitt.

4.2 Förvaltning av administrativa medarbetaruppdrag

Varje organisation ansvarar för sin information, vilket även innefattar administrativa medarbetaruppdrag. Det innebär ansvar för vilka personer som är kopplade till uppdragen under vilken tid samt vilka rättigheter (behörighetsområdesegenskaper) som medarbetaruppdraget innehåller.

5. Exempel på användning av administrativa medarbetaruppdrag för behörighetsstyrning

5.1 Hitta och jämför vård / Kontaktskortsadmin

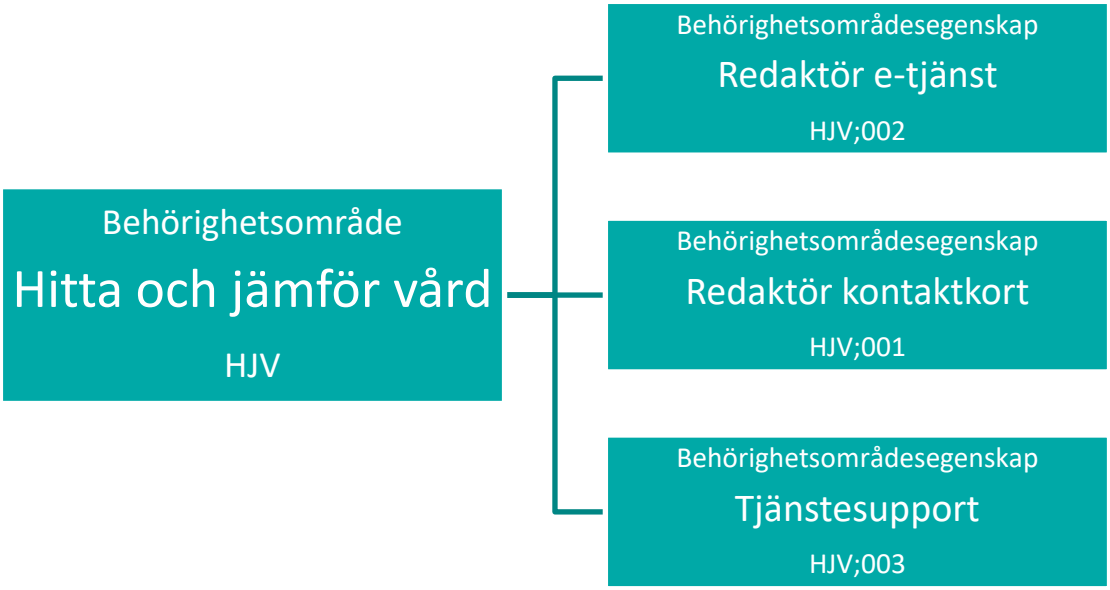
Hitta och jämför vård är den del på 1177.se som presenterar kontaktinformation till landets vårdmottagningar, deras vårdutbud och vårdkvalitet. Varje enskild mottagning har ett eget ”Kontaktkort” där kontaktuppgifter, e-tjänster och övrigt utbud presenteras. Informationen på kontaktkorten kommer primärt från HSA men det finns också möjlighet att komplettera med information som inte finns i HSA (t.ex. utbud, erbjudna e-tjänster) via det administrativa verktyget Kontaktkortsadmin (KKA). Åtkomst till KKA regleras med administrativa medarbetaruppdrag.

I behörighetsområdet för ”Hitta och jämför vård” har det skapats tre behörighetsområdesegenskaper som styr vad användaren får göra i verktyget. Dessa behörighetsområdesegenskaper är:

- *Redaktör e-tjänst:* Ger behörighet att skapa och redigera information på fliken ”Presentera e-tjänster” i Kontaktskortsadmin.

- *Redaktör kontaktkort:* Ger behörighet att skapa och redigera information i flikarna ”Vårt utbud”, Registrera e-tjänster”, ”Aktuellt” och ”Läs mer”.

- *Tjänstesupport:* Behörighet för Inera att kunna stödja och ge support till anslutna organisationer. Denna behörighetsområdesegenskap har en begränsning som gör att den endast kan registreras på administrativa medarbetaruppdrag under Inera AB.



Figur 5 Behörighetsområde "Hitta och jämför vård".