

# Uppdrag att ta fram och tillgängliggöra en sammanhållen infrastruktur för identitet och behörighet inom hälso- och sjukvården

Slutredovisning av regeringsuppdrag enligt E-hälsomyndighetens regleringsbrev 2025

EHM 2025/00348



Denna publikation skyddas av upphovsrättslagen.

Citera gärna rapporten men uppge alltid källa: Rapportens namn, år och E-hälsomyndigheten.

Publicerad: E-hälsomyndigheten, december, 2025.

Diarienummer: 2025/00348

Adress: Södra Långgatan 60, Kalmar

Sankt Eriksgatan 117, Stockholm

E-post: [registrator@ehalsomyndigheten.se](mailto:registrator@ehalsomyndigheten.se)

Telefon: 010-458 62 00

[www.ehalsomyndigheten.se](http://www.ehalsomyndigheten.se)

## Förord

Regeringen gav E-hälsomyndigheten i regleringsbrevet för 2025 i uppdrag att ta fram och tillgängliggöra en sammanhållen infrastruktur för identitet och behörighet inom hälso- och sjukvården.

Denna rapport utgör den slutliga redovisningen och ska enligt uppdraget redovisas senast den 12 december 2025 till Regeringskansliet (Socialdepartementet).

Beslut om den här rapporten har fattats av generaldirektör Gunilla Nordlöf.

Uppdragsledare Niklas Dahlbäck har varit föredragande. I den slutliga handläggningen har avdelningschef Peter Alvinsson och sektionschef Camilla Björk deltagit.

Gunilla Nordlöf

Generaldirektör

# Sammanfattning

E-hälsomyndighetens har fått i uppdrag av regeringen att ta fram och tillgängliggöra en sammanhållen infrastruktur för identitet och behörighet inom hälso- och sjukvården.<sup>1</sup>

Myndigheten för digital förvaltning (Digg) har fått i uppdrag att ta fram och utveckla en sammanhållen infrastruktur för identitets- och behörighetshantering inom ramen för Ena – Sveriges digitala infrastruktur. Arbetet ska ske i nära samverkan med E-hälsomyndigheten.<sup>2</sup>

En nationell identitets- och behörighetsinfrastruktur ska bidra till en säker och effektiv datadelning samt minska behörighetsadministration hos vårdgivare och belastning på användare. Den kan även bidra till ökad patientsäkerhet och integritetsskydd för patienter. Vidare ska infrastrukturen bidra till nationell interoperabilitet och högre tillit till den nationella digitala infrastrukturen för hälso- och sjukvården.

För att ge användare hos en organisation tillgång till hälsodata hos andra organisationer krävs hög nivå av tillit mellan organisationerna avseende den information som ligger till grund för åtkomst. Idag saknas en nationell gemensam lösning inom hälso- och sjukvården där vårdgivare och andra organisationer på ett effektivt sätt kan nå denna tillit. Det finns även problematik idag inom hälso- och sjukvården där olika system har olika sätt att tekniskt och administrativt lösa identitets- och behörighetshantering, vilket leder till ineffektivitet för vårdpersonal och vårdgivare.

E-hälsomyndigheten och Digg har under 2025, tillsammans med bland andra Inera, Internetstiftelsen och regioner, arbetat för att beskriva hur identitet- och behörighetsinfrastrukturen inom Ena ska fungera.

Lösningen baseras på en federation, vilket är en skalbar gemensam infrastruktur där ingående organisationer kan nå tillit till behörighetsgrundande information, det vill säga, den information som ligger till grund för begäran om åtkomst från en annan organisation. Detta innefattar användares identitet. Lösningen innefattar bland annat tekniska ramverk och specifikationer, anslutningsregler och anslutningsprocesser.

E-hälsomyndigheten bedömer att identitet- och behörighetsinfrastrukturen kan tillämpas på den nationella digitala infrastrukturen (NDI) inom hälso- och sjukvården, som

---

<sup>1</sup> Regleringsbrev för budgetåret 2025 avseende E-hälsomyndigheten (S2025/01234)

<sup>2</sup> Regleringsbrev för budgetåret 2025 avseende Myndigheten för digital förvaltning (Fi2024/00591 och Fi2024/02483 (delvis))

E-hälsomyndigheten har i uppdrag att genomföra<sup>3</sup>, och Nationella läkemedelslistan, samt för att kunna realisera införandet av det europeiska hälsodataområdet (EHDS).

Infrastrukturen baseras på den lösning som Digg ansvarar för att tillhandahålla. När den ska tillämpas för behörighetshantering där tillit krävs mellan organisationer, behöver vissa sektorsspecifika kompletteringar göras.

E-hälsomyndigheten bedömer att infrastrukturen har etablerats i den omfattning att anslutande organisationer, såsom vårdgivare och leverantörer av legitimeringstjänster samt operatörer, kan påbörja analys för anpassning och anslutning till infrastrukturen. Vidare bedömer E-hälsomyndigheten att det under 2026 kommer vara möjligt för aktörer inom hälso- och sjukvården att ansluta, men det kräver att operatörer har anslutit till infrastrukturen och att de rättsliga förutsättningar som Digg identifierat för den sektorsöverskridande infrastrukturen finns på plats.

Fortsatt aktivt arbete krävs hos E-hälsomyndigheten, Digg och andra organisationer för att infrastrukturen ska tillämpas, förvaltas och vidareutvecklas. E-hälsomyndigheten föreslår därför att myndigheten får i uppdrag att fortsatt tillgängliggöra infrastrukturen för användning inom hälso- och sjukvården. Detta förutsätter att myndigheten innehar rollen som federationsområdesansvarig. Uppdraget ska bland annat utreda de rättsliga förutsättningarna för att vara federationsområdesansvarig. Uppdraget behöver även ta fram vissa sektorsspecifika kompletteringar för delar som den sektorsöverskridande infrastrukturen inte tillhandahåller och utreda rättsliga förutsättningar för dessa kompletteringar. Kompletteringarna innefattar bland annat att ta fram tillitsmärken, tillse efterlevnadskontroller av tillitsmärken och att etablera anslutningsoperatörer. Uppdraget ska också omfatta stöd till anslutande organisationer.

E-hälsomyndigheten föreslår att Socialstyrelsens register över legitimerad hälso- och sjukvårdspersonal och personal med bevis om rätt att använda yrkestiteln undersköterska (HOSP) ska tillgängliggöras, via API och e-tjänst, till organisationer inom hälso- och sjukvården som har behov av att använda registret för behörighetstilldelning eller behörighetskontroller. E-hälsomyndigheten föreslår också att information om personer med särskilt förordnande tillgängliggörs på liknande sätt. I dag är inte uppgifter i HOSP eller uppgifter om särskilda förordnanden digitalt tillgängliga för alla de aktörer inom hälso- och sjukvårdssektorn som skulle ha nytta av den, avseende behörighetstilldelning

---

<sup>3</sup> Uppdrag om att genomföra en nationell digital infrastruktur i hälso- och sjukvården och förbereda för att Sverige ska genomföra förordningen om det europeiska hälsodataområdet (EHDS) rörande primäranvändning, S2024/02156 (delvis)

och behörighetskontroll. Tillgängliggörande av dessa uppgifter skulle bidra till ökad säkerhet inom sektorn.

# Innehåll

Förord .....	3
Sammanfattning .....	4
Innehåll.....	7
1 Inledning och beskrivning av uppdraget .....	9
1.1 Bakgrund och uppdraget .....	9
1.2 Syfte, mål och effekt.....	9
1.3 Avgränsningar.....	10
1.4 Ena - Sveriges digitala infrastruktur .....	11
1.5 Identitet- och behörighetshantering idag inom hälso- och sjukvård .....	12
1.6 Prioriterat område för regioner och kommuner.....	13
1.7 Ökat behov av identitets- och behörighetsinfrastruktur med anledning av EHDS och nationell digital infrastruktur .....	14
1.8 Olika förutsättningar kräver flexibel lösning .....	14
2 Genomförande .....	15
2.1 Arbetsprocess och aktiviteter .....	15
2.2 Samverkan.....	15
2.3 Uppnådda leveranser.....	16
2.4 Identifierade utmaningar under genomförandet.....	17
2.5 Metoder för kvalitetssäkring .....	17
3 Resultat.....	20
3.1 Federativ infrastruktur .....	20
3.2 Infrastrukturen ska stödja olika typer av scenarion.....	21
3.3 Infrastrukturens utformning .....	21
4 Användning av infrastrukturen inom hälso- och sjukvård.....	28
4.1 Hur förhåller sig infrastrukturen till dagens situation.....	28
4.2 Tillitstruktur för sektorns behov .....	29
4.3 Identitet- och behörighetshantering i EHDS och andra nationella behov .....	29
4.4 Nationella läkemedelslistan.....	33

4.5 Roller i infrastrukturen .....	34
4.6 Robusthet och tillgänglighet.....	35
4.7 Rättsliga förutsättningar .....	36
5 Överväganden och förslag.....	37
5.1 Tillgängliggöra HOSP och information om särskilda förordnanden .....	37
5.2 Rekommendation till fortsatt arbete.....	39
6 Konsekvensanalys.....	40
6.1 Konsekvenser för hälso- och sjukvården.....	40
6.2 Konsekvenser för individen.....	40
6.3 Konsekvenser för E-hälsomyndigheten .....	41

# 1 Inledning och beskrivning av uppdraget

## 1.1 Bakgrund och uppdraget

I regleringsbrevet för 2025 gavs E-hälsomyndigheten i uppdrag att ta fram och tillgängliggöra en sammanhållen infrastruktur för identitet och behörighet inom hälso- och sjukvården.<sup>4</sup> Arbetet ska ske i samverkan med Myndigheten för digital förvaltning (Digg) och det förvaltningsgemensamma arbetet inom ramen för Ena – Sveriges digitala infrastruktur. Denna rapport utgör E-hälsomyndighetens slutredovisning av uppdraget.

Regeringen gav samtidigt Digg i uppdrag att utveckla en sammanhållen infrastruktur för identitets- och behörighetshantering, som ska kunna tillhandahållas inom ramen för Ena – Sveriges digitala infrastruktur. Uppdraget ska utföras i nära samverkan med E-hälsomyndigheten för att möta behovet av att införa en nationell digital infrastruktur i hälso- och sjukvården (NDI), inklusive Nationella läkemedelslistan. Digg ska inom ramen för uppdraget analysera behovet av och lämna förslag på författningsändringar samt föreslå hur infrastrukturen fortsatt ska förvaltas och drivas, även i kris och krig.

## 1.2 Syfte, mål och effekt

För att ge patienter och användare hos en organisation tillgång till hälsodata hos andra organisationer krävs hög nivå av tillit mellan organisationerna avseende den information som ligger till grund för åtkomst. Idag saknas en nationell gemensam lösning inom hälso- och sjukvården där vårdgivare och andra organisationer på ett effektivt sätt kan nå denna tillit.

Det finns även problematik idag inom hälso- och sjukvården där olika system har olika sätt att tekniskt och administrativt lösa identitets- och behörighetshantering. Denna fragmentering medför ineffektivitet, bland annat på grund av att personal behöver lägga mycket tid på att logga in i olika system<sup>5</sup> och att vårdgivares administration av behörighetskällor tar mycket tid.

Syftet med E-hälsomyndighetens uppdrag är bidra till säker och effektiv datadelning inom hälso- och sjukvården. Detta görs genom att tillgängliggöra en sammanhållen infrastruktur för identitets- och behörighetshantering inom sektorn. Infrastrukturen ska möjliggöra tillit till behörighetsgrundande information, inklusive uppgifter om identiteter,

---

<sup>4</sup> Regleringsbrev för budgetåret 2025 avseende E-hälsomyndigheten (S2025/01234)

<sup>5</sup> Vårdförbundet (2025) *Den dumma digitaliseringen – En studie om sjuksköterskors digitala arbetsmiljö*

som förmedlas mellan aktörer, vilket skapar förutsättningar för säkra åtkomstkontroller. Uppdraget syftar också till att minska problemet med den fragmenterade hanteringen av identitet och behörighet i vårdgivarnas system.

Föreliggande uppdrag behöver särskilt fokusera på sektorns behov avseende behörighetshantering. Identitetshanteringen är mer av förvaltningsgemensam karaktär och hanteras främst genom det uppdrag Digg har.

Uppdraget har följande effektmål.

- **Högre tillit till den nationella digitala infrastrukturen i hälso- och sjukvården:** Lösningen ska öka tilliten hos vårdgivare, patienter och andra intressenter genom att implementera en robust och transparent lösning för identitets- och behörighetskontroll.
- **Nationell interoperabilitet:** Lösningen ska fungera för alla vårdgivare, oavsett finansiering.

Uppdraget skapar även förutsättningar att nå vissa effekter. Den infrastruktur som uppdraget ska tillhandahålla behöver tillämpas av aktörer inom hälso- och sjukvården för att effekterna ska uppnås. Detta möjliggörs genom användning av standarder och enhetliga tekniska ramverk och gemensamma tillitsstrukturer.

- **Effektiv datadelning:** En gemensam identitets- och behörighetshantering i sektorn möjliggör effektiv delning av data mellan olika system och organisationer, både offentliga och privata aktörer.
- **Förbättrad patientsäkerhet och ökat integritetsskydd för patienter:** Ökad möjlighet att säkerställa att endast behörig personal har tillgång till känslig patientinformation.
- **Ökad effektivitet inom hälso- och sjukvården:** Minska onödig tid som personal behöver lägga på att till exempel logga in i olika system.
- **Minskad administrativ börda inom vården:** Minska administration av användarkonton och behörighetshantering hos vårdgivare.

### 1.3 Avgränsningar

Uppdraget omfattar inte att ta fram behörighetsregler för delning av data mellan organisationer, såsom vilken vårdpersonal som får ha åtkomst till olika informationsmängder. Den infrastruktur som uppdraget etablerar ska dock kunna användas för bland annat den nationella digitala infrastrukturen i hälso- och sjukvården (NDI) samt för införandet av det europeiska hälsodataområdet (EHDS).

Uppdraget omfattar inte generella förbättringar rörande identitetshandling, såsom problematik kring reservnummer och identitetsmatchning.

Eftersom uppdraget handlar om att tillgängliggöra en infrastruktur omfattar uppdraget inte själva anslutningsarbetet till infrastrukturen. Däremot ska förutsättningar för anslutning beskrivas.

Uppdraget innebär nödvändigtvis inte att infrastrukturen är fullt skalbar vid tidpunkten för slutredovisning av uppdraget. Detta förutsätter arbete hos kommande operatörer inom federationen. E-hälsomyndigheten kan inte fullt ut styra över dessa aktörers anslutningsarbete. Etablering av infrastrukturen sker dock i nära samarbete med tilltänkta operatörer såsom Inera AB och Internetstiftelsen.

E-hälsomyndigheten tar inte fram förslag på författningsändringar då detta hanteras inom ramen för det uppdrag Digg fått.

## 1.4 Ena - Sveriges digitala infrastruktur

Den sammanhållna infrastrukturen för identitets- och behörighetshandling ska kunna tillhandahållas inom ramen för Ena – Sveriges digitala infrastruktur. Ena är en nationell resurs som syftar till att möjliggöra smartare digitalisering av offentlig sektor, underlätta för offentlig sektor att dela data och att bygga digitala lösningar som fungerar bättre för invånare och företag, samtidigt som kostnaderna för digitalisering minskar. De olika lösningarna inom Ena har tagits fram och förvaltas av olika myndigheter. Digg ansvarar för samordningen av Ena.

Flera av lösningarna inom Ena är inte synliga för slutanvändaren eftersom de utgör den underliggande digitala infrastrukturen som andra aktörer nyttjar för att skapa bättre digitala tjänster för användare. Därmed bidrar lösningarna till bättre samhällsservice hos myndigheter, samt främjar innovation och tillväxt.

Samordnad identitet och behörighet, vilket är en infrastruktur inom Ena för identitet och behörighetshandling, är en sådan underliggande infrastruktur som ska säkerställa att rätt medarbetare eller organisation får tillgång till rätt information vid rätt tillfälle. Genom att erbjuda en sådan lösning inom Ena, kan aktörer använda lösningens gemensamma regler och tekniska komponenter för handtering av identitet och behörighet. Detta möjliggör bättre interoperabilitet både inom och mellan olika verksamhetsområden.

Genom att bygga ut den nya infrastrukturen successivt etableras en stabil grund som fler aktörer kan ansluta till. Detta leder på sikt till att hela den offentliga sektorn ges bättre förutsättningar att utveckla effektiva och säkra digitala tjänster.

## 1.5 Identitet- och behörighetshantering idag inom hälso- och sjukvård

Hantering av digitala identiteter och styrning av behörigheter har inom hälso- och sjukvård i Sverige byggts upp organiskt. Detta har inneburit att kravställningen är framtagen utifrån en organisations eller en tjänsts behov. Därav finns det många olika kravställningar och lösningar som ofta är snarlika men inte direkt kompatibla. Detta leder till bristande interoperabilitet, bristande skalbarhet och ökade kostnader. Ekosystemet består då av en mer komplex infrastruktur och förvaltning med olika integrationslösningar att förhålla sig till.

Dagens system använder således olika lösningar för att kontrollera och hantera identiteter och behörigheter. Dessa system tillhandahålls dessutom av många olika aktörer med separata tekniska plattformar, vilket i vissa fall skapar hinder för digital samverkan. Exempelvis så finns det idag många olika federationer, som Sweden Connect, Sambis, Hälso- och sjukvårdens adressregister (HSA) med flera, som inte samverkar. Det innebär bland annat att kommunerna behöver ingå i flera olika federationer då till exempel det kommunala skoluppdraget omfattar både elevhälsa och skolverksamhet som tillhör separata federationer. Dessutom hänvisas även privata aktörer utan offentlig finansiering ofta till egna lösningar och samverkansformer då det finns offentliga aktörer som inte upplåter sin infrastruktur till privata aktörer.

Det finns idag en fungerande marknad för identifiering. Identitetsfederationen Sweden Connect är etablerad och fungerande, dock med vissa begränsade möjligheter för privata aktörer att få ansluta sina legitimeringstjänster. Inera lanserade den 30 september 2025 en ny legitimeringstjänst som följer tillitsramverket för Svensk e-legitimation.<sup>6</sup>

Behörighet är ett område med stor komplexitet och ett flertal olika lösningar. Genom en gemensam referensarkitektur, där man tydligt skiljer på aktörer och digitala tjänsters ansvar, skapar man förutsättningar för att olika lösningar kan samexistera och fungera ihop, det vill säga bygga broar mellan lösningarna. Ett exempel på det är Ineras *Referensarkitektur för identitet och åtkomst*<sup>7</sup> som stipulerar en tydlig skiljelinje mellan digital tjänst, identitet och åtkomst via attributskällor. Identitetsintygsutfärdare är navet, med lösa kopplingar till de digitala tjänsterna och attributskällorna. Kopplingarna bygger på standardiserade kommunikationsprotokoll.

---

<sup>6</sup> Myndigheten för digital förvaltning *Tillitsramverk för Svensk e-legitimation*

<sup>7</sup> Inera *Referensarkitektur för Identitet och åtkomst, Revision B*

Många digitala tjänster hanterar dock fortfarande identitet och behörighet internt inom respektive aktör och digital tjänst med kopplingar till olika attributkällor. Det är även vanligt förekommande att digitala tjänster hämtar information för en och samma medarbetare från flera olika källor, där personen alltså finns registrerad på flera ställen för syftet behörighetsstyrning, vilket i många fall orsakar onödig dubbelregistrering och högre förvaltningskostnader.

Det finns ett stort behov av att skapa en tillitsstruktur mellan aktörer, sektorer, digitala tjänster och attributskällor på nationell nivå, för att möjliggöra att flera parallella lösningar kan samverka.

## 1.6 Prioriterat område för regioner och kommuner

Förbättrad identitets- och behörighetshantering är ett av de prioriterade initiativen inom *Handslag för digitalisering*<sup>8</sup> som Sveriges kommuner enats om. Initiativet genomförs tillsammans med Sveriges kommuner och regioner (SKR), Adda<sup>9</sup> och Inera. Syftet med initiativet är att skapa en tydlighet i hur kommuner bör etablera och arbeta med identitets- och behörighetslösningar för fortsatt säker och effektiv verksamhet.

I regionernas *10-punktslista för Nationell digital infrastruktur för hälso- och sjukvården*<sup>10</sup> konstateras att Sverige behöver en identitets- och behörighetsfederation där offentliga aktörer inom stat, region och kommun, såväl som privata aktörer inom det offentliga uppdraget ingår. Regionerna anser att regeringen och regionerna bör säkerställa att

- Utformningen av en nationell identitets- och behörighetsfederation genomförs
- Federationen omfattar hela den offentliga förvaltningen inklusive privata utförare samt system-till-system-kommunikation

E-hälsomyndighetens uppdrag kommer att hantera många av de behov som regioner och kommuner anser är centrala, vilket innefattar båda punkterna ovan. E-hälsomyndighetens uppdrag inkluderar att ta fram en infrastruktur som även kan användas av privata utförare utanför det offentliga uppdraget.

---

<sup>8</sup> SKR (2023) *Kommungemensamt handslag för välfärdsutveckling genom digitalisering*

<sup>9</sup> Adda är ett företag som ägs av SKR och majoriteten av Sveriges kommuner.

<sup>10</sup> SKR (2024) *10-punktslista för Nationell digital infrastruktur för hälso- och sjukvården*

## 1.7 Ökat behov av identitets- och behörighetsinfrastruktur med anledning av EHDS och nationell digital infrastruktur

Det europeiska hälsodataområdet (EHDS) ställer nya krav på hur vården i Europa och Sverige ska hantera hälsodata och omfattar alla vårdsektorns både offentliga och privata aktörer. Detta stärker således behovet av en interoperabel identitets- och behörighetsinfrastruktur så att svenska lösningar för elektronisk identifiering (eID), behörighetshantering och betrodda tjänster fungerar sömlöst på ett skalbart och effektivt sätt både nationellt och inom EU. Behovet finns både för att möta de krav som EHDS-förordningen ställer och för att ge förutsättningar för införandet av nationell digital infrastruktur inom hälso- och sjukvården (NDI).

eIDAS-förordningen<sup>11</sup> skapar redan idag en ram för gränsöverskridande digital identifiering. Dock finns det krav inom EHDS på att hälsodata ska vara sökbart gränsöverskridande på respektive hemlands identitet vilket inte är möjligt i dagens lösningar.

Det finns i dagsläget ingen samlad bild av vilka behörighetsstyrande informationsmängder som är nödvändiga för utbyte mellan medlemsstaterna inom EU, vilket dock kommer att klargöras efter färdigställandet av genomförandeakterna för EHDS-förordningen.

## 1.8 Olika förutsättningar kräver flexibel lösning

Vårdsektorn i Sverige består av en mycket varierad aktörsstruktur, med allt från enmansföretag och små mottagningar till stora regioner, vårdkoncerner, apotekskedjor och myndigheter. Även kommuner ingår och dessa varierar i storlek, men är i de flesta fall förhållandevis små jämfört med regioner och vissa privata aktörer. Aktörerna har i stor utsträckning skilda organisatoriska, tekniska och ekonomiska förutsättningar att delta i gemensamma infrastrukturlösningar.

För att en identitets- och behörighetsfederation ska kunna fungera i praktiken krävs därför en flexibel och skalbar modell som tar höjd för denna variation. Lösningen måste tillåta olika nivåer av teknisk integration, anslutningsformer och efterlevnadskontroll, samtidigt som den bygger på gemensamma lösningar och regler för tillit, säkerhet och interoperabilitet.

---

<sup>11</sup> Förordning om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden

För att uppnå en nationellt sammanhållen lösning krävs ett ramverk som möjliggör deltagande för hela vårdsektorn, inklusive både offentliga och privata aktörer, oavsett storlek och typ av aktör, utan att tilliten påverkas negativt.

En framgångsrik identitets- och behörighetsfederation förutsätter därmed en varierad men enhetligt styrd infrastruktur, där flexibilitet inte blir ett hinder för säkerhet, utan en förutsättning för inkludering och långsiktig hållbarhet.

## 2 Genomförande

### 2.1 Arbetsprocess och aktiviteter

Uppdragets arbete är till största del ett gemensamt arbete tillsammans med andra organisationer. Det har varit centralt att etablera effektiva samverkansstrukturer. Inom Ena finns en operativ arbetsgrupp som arbetar med etablering av Samordnad identitet och behörighet. Inom arbetsgruppen har olika leveransteam etablerats med fokus på digital samverkan, tillitsstruktur, federationsinfrastruktur, verksamhet och juridik.

E-hälsomyndigheten eller Digg har varit sammankallande för respektive leveransteam.

Ena arbetsutskott har använts för styrning av arbetet. I detta utskott ingår E-hälsomyndigheten, Digg, SKR, Inera, Internetstiftelsen, Sunet, Region Stockholm och Skolverket.

För att få snabb återkoppling på leveranser har uppdraget arbetat hypotesdrivet. Hypoteser och antaganden har tidigt formulerats så att deltagande organisationer kan ge synpunkter på leveranserna. Leveransteamen har tagit fram hypoteser som sedan lyfts till övriga deltagare i Enas arbetsgrupp.

Uppdragets ambition har varit att resultatet ska mynna ut i en praktisk tillämpbar lösning, varför arbetet i största möjliga mån ska verifieras i praktiska tillämpningar tillsammans med berörda aktörer. Därför har ett pilotarbete, initialt i testmiljö, med anslutande aktörer etablerats, för att använda Ena för anslutning till Nationella läkemedelslistan.

### 2.2 Samverkan

Infrastrukturen baseras på Enas Samordnad identitet och behörighet, som ska vara en förvaltningsgemensam lösning. E-hälsomyndighetens roll i framtagandet av federationsinfrastrukturen är att säkerställa att hälso- och sjukvårdens behov tillgodoses.

Inom ramen för Ena har uppdraget samarbetat med flera organisationer, inklusive Digg, Inera, Internetstiftelsen, Sveriges kommuner och regioner, Västra götalandregionen och Region Stockholm.

Utöver samarbetet med Digg har etablering av infrastrukturen skett i nära samarbete med de tilltänkta operatörerna Inera och Internetstiftelsen. De har under en lång tid utvecklat och tillhandahållit tjänster för säker digital samverkan inom vården.

Förslag har även förankrats med organisationer som inte ingår i Ena-arbetsgrupp. Dialog har även förts med systemleverantörer. Bland annat har en leverantörsdag genomförts där leverantörer av vårdinformationssystem och identitets- och behörighetssystem (IAM-system) har bjudits in för att få information om och ge synpunkter på tekniska delar i infrastrukturen.

## 2.3 Uppnådda leveranser

E-hälsomyndigheten har under 2025, inom ramen för Ena, tillsammans med andra deltagande organisationer levererat beskrivning av infrastrukturen inom följande områden.

### 2.3.1 Digital samverkan

Digital samverkan handlar om hur de system som organisationer anslutit till infrastrukturen ska kommunicera gällande identitet och behörighet. Detta beskrivs till största del genom tekniska specifikationer.

### 2.3.2 Tillitsstruktur

Grunden i en federationsinfrastruktur bygger till stor del på att kunna uppnå tillit till de organisationer som anslutit sina system. Inom leveransområdet tillitsstruktur har beskrivningar av tillitsskapande objekt, funktioner och krav tagits fram. Detta ligger till grund för etablering av tekniska och administrativa lösningar som möjliggör tillit mellan anslutna organisationer.

### 2.3.3 Federationsinfrastruktur

Detta område beskriver hur de centrala delarna av infrastrukturen fungerar. Teknisk lösning för hantering av information om anslutna organisationer inom infrastrukturen har beskrivits. Området innefattar även beskrivning av vilka roller som finns, såsom olika typer av operatörer och deras ansvar.

### 2.3.4 Verksamhet och juridik

För att infrastrukturen ska fungera i praktiken krävs etablering av verksamhet hos många aktörer. Inom detta leveransområde har bland annat anslutningsprocesser beskrivits. Arbete rörande kommunikationsarbete och samverkansstrukturer har påbörjats.

Digg har i uppdrag att ge förslag på författningsändringar. I det juridiska arbetet har även en roll- och ansvarsmodell tagits fram.

### 2.3.5 Pilot

En pilot har genomförts i testmiljö där en system- och tjänsteleverantör inom omsorg har anslutit till Nationella läkemedelslistan. Piloten visade att den tekniska lösning som föreslagits fungerade väl. Mer om piloten beskrivs i avsnitt 2.5 *Metoder för kvalitetssäkring*.

## 2.4 Identifierade utmaningar under genomförandet

En faktor som bidragit till komplexitet i arbetet är att infrastrukturen behöver stödja många olika typer av aktörer och mönster. Många perspektiv måste belysas för att komma fram till en ändamålsenlig och effektiv lösning.

Det finns även behov av att beakta nuvarande situation kring identitets- och behörighetshantering inom hälso- och sjukvården. Stora investeringar har gjorts inom detta område och det är viktigt att kunna dra nytta av dessa även i en förflyttning till den nya infrastrukturen.

En styrka i arbetet har varit aktivt deltagande från många organisationer, men det har också inneburit en utmaning gällande att nå samsyn i detaljer i lösningen.

Lösningen har beroende till den internationella standarden OpenID Federation (OIDF). Denna standard är under utveckling och det innebär vissa utmaningar rörande fastställande av lösningens tekniska delar.

## 2.5 Metoder för kvalitetssäkring

Uppdraget har använt flera metoder för att kvalitetssäkra leveranser. Gemensamt för dessa är involvering av andra organisationer. E-hälsomyndigheten och Digg har tillsammans bedrivit kvalitetssäkringsarbetet.

## 2.5.1 Förankring i Ena-arbetsgrupp

Inom Ena arbetsgrupp deltar flera organisationer aktivt med framtagande och granskning av specifikationer, övrig dokumentation och tekniska lösningar. Arbetsgruppen och dess underliggande leveransteam har använts för kvalitetssäkring av dessa leveranser.

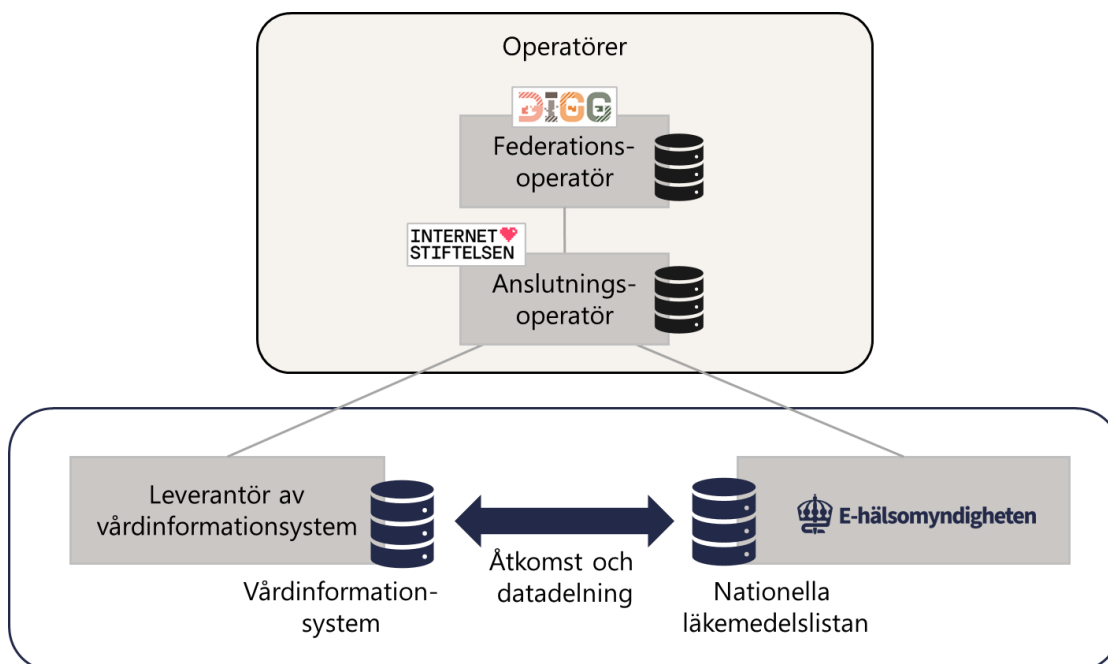
## 2.5.2 Pilot

Ena arbetsutskott enades om att Nationella läkemedelslistan (NLL) skulle användas som ett pilotfall för praktisk tillämpning av infrastrukturen. Målet med pilotarbetet var att ett antal vårdaktörer skulle integrera sina system med NLL genom Enas federationsinfrastruktur Samordnad identitet och behörighet. Detta arbete innebar att E-hälsomyndigheten, som tillhandahåller NLL, samt deltagande vårdaktörer behöver ansluta till federationsinfrastrukturen.

Fokus för piloten var att kvalitetssäkra leveranser inom digital samverkan och federationsinfrastruktur, det vill säga, en teknisk inriktad aktivitet. Gällande tillitsstrukturer valdes att använda befintlig tillit till deltagande organisationer, som redan ingår i identitets- och behörighetsfederationen Sambi.

En system- och tjänsteleverantör inom vården utvecklade sin behörighetslösning och anslöt denna, samt sitt vårdinformationssystem, till federationsinfrastrukturen i testmiljö. E-hälsomyndigheten anpassade sin åtkomstlösning för NLL och anslöt denna. I testmiljön genomfördes ett antal tester där användare av vårdinformationssystemet läste information från NLL. I testerna ingick även teknisk integration med anslutningsoperatören Internetstiftelsen. Testerna föll väl ut.

Figur 1. Deltagande parter i pilottesterna



Notera att denna pilot avser en viss typ av tillämpning. Till stora delar kommer det mönster som testas i piloten att vara aktuellt även för andra typer av datadelningar inom sektorn, men det kan finnas skillnader.

E-hälsomyndigheten anser att pilotarbete är värdefullt och kommer därför verka för ytterligare pilotfall. E-hälsomyndigheten anser att, när förutsättningar finns, ska även piloter i produktionsmiljö genomföras.

Se avsnitt 3.3.1 *Roller och ansvar* för vidare beskrivning av de olika rollerna.

### 2.5.3 Proof-of-concept-implementation

Som ett led i att förbereda inför piloten har E-hälsomyndigheten även tagit fram en proof-of-concept (PoC). Denna PoC innehåller samma komponenter som piloten, men med den skillnad att det är E-hälsomyndigheten som tar fram och tillhandahåller samtliga komponenter. Detta innebär att det inte krävs att pilotaktörer finns tillgängliga för att kunna genomföra tester.

Syftet med denna PoC är dels att vara kompetensbyggande inom myndigheten, och dels att i ett tidigt skede kunna kvalitetssäkra de mönster och specifikationer som tas fram inom Samordnad identitet och behörighet. Den har också en roll i att kunna skapa ha en god samverkan med de aktörer som ingår i piloten. Där används denna PoC som underlag

att diskutera vad som tekniskt förväntas av pilotaktörer genom att kunna demonstrera hela flödet som ska byggas inom piloten. På detta sätt fungerar denna PoC i viss mån som en referensimplementation till piloten.

## 2.5.4 Leverantörsdialog

I september 2025 genomfördes en leverantörsdag där leverantörer av vårdinformations-system och identitets- och behörighetssystem bjöds in. Dessa leverantörer är centrala för att infrastrukturen ska bli så enkel som möjligt att införa. Arbetsgruppen i Ena, där E-hälsomyndigheten, Digg, Inera och Internetstiftelsen ingår, presenterade förslag till tekniska specifikationer. Leverantörerna har även fått tillgång till dessa specifikationer och har möjlighet att ge synpunkter.

# 3 Resultat

## 3.1 Federativ infrastruktur

Infrastrukturen baseras på en federativ modell genom Enas Samordnad identitet och behörighet. Federationer finns visserligen redan, men den som nu föreslås avses bli ett ekosystem där många fler aktörer, så väl offentliga som privata, tillsammans skapar förutsättningar för en nationell, säker, tillförlitlig och effektiv digital infrastruktur.

Syftet med en federativ infrastruktur är följande.

- Göra det möjligt för självständiga organisationer att samverka digitalt och samtidigt behålla sitt eget ansvar
- Skapa en gemensam och enhetlig grund för hur identitets- och behörighetsinformation hanteras
- Genom gemensamma regler och specifikationer möjliggöra förtroende mellan aktörer så att information kan delas på ett säkert och rättssäkert sätt
- Säkerställa att aktörer samverkar enligt gemensamma spelregler men förblir självständiga i sina uppdrag

Skalbarheten är central. Den möjliggör att roller kan fördelas mellan olika aktörer, att tekniska delar kan utvecklas och förvaltas separat samt att nya funktioner successivt kan läggas till.

Genom denna utformning kan den föreslagna infrastrukturen anpassas till ändrade behov, stödja innovation och samtidigt utformas så att den blir robust och pålitlig över tid.

En grundläggande inriktning är att återanvända befintliga arkitekturer och regelverk där det är möjligt och att bygga vidare på etablerade standarder.

För att en federation ska fungera krävs en infrastruktur, det vill säga den praktiska uppsättning av komponenter som gör samverkan möjlig. Infrastrukturen omfattar tekniska system, roller, regler och avtal som tillsammans ger förutsättningar för en säker och effektiv samverkan.

## 3.2 Infrastrukturen ska stödja olika typer av scenarion

Infrastrukturen för identitet och behörighetshantering kan användas för olika typer av scenarion där tillgång till information behövs. Infrastrukturen kan användas i de fall användare behöver tillgång till information, såsom medarbetare hos en vårdgivare eller en privatperson. Den kan även användas vid kommunikation mellan olika enheter i automatiserade processer, även kallat maskin-till-maskin eller tekniska gränssnitt. Detta inkluderar fallet då system hos en organisation ska ha åtkomst till system hos en annan organisation.

## 3.3 Infrastrukturens utformning

Federationsinfrastrukturen utgörs av ett distribuerat nätverk där flera aktörer samverkar för att möjliggöra säker och effektiv digital samverkan mellan organisationer. Varje aktör bidrar med sina egna komponenter och tjänster, men följer gemensamma regler och specifikationer, som säkerställer att allt fungerar tillsammans som en helhet.

Infrastrukturen är utformad för att vara decentraliserad, skalbar och robust, vilket gör att den kan växa och förändras över tid utan att förlora stabilitet eller förutsägbarhet. Genom den decentraliserade modellen kan ansvar och funktioner fördelas mellan flera parter. Ingen enskild aktör kontrollerar helheten, utan styrningen sker genom gemensamma och överenskomna regler, specifikationer och processer. Detta skapar en flexibel struktur som kan anpassas till olika behov. Nya tjänster, komponenter eller samverkansområden kan läggas till stegvis och integreras med befintliga delar.

Federationsinfrastrukturen bygger på den öppna internationella specifikationen OpenID Federation (OIDF) som beskriver hur olika protokoll för identitets- och behörighetskontroll, såsom OpenID Connect, OAuth 2.0 och SAML<sup>12</sup>, ska användas för att skapa interoperabilitet. Dessa internationella specifikationer är generella och lämnar stort utrymme för tolkning. De utgör därför en gemensam grund som behöver

---

<sup>12</sup> SAML behöver utökas för att kunna användas

kompletteras för att skapa en fungerande federationsinfrastruktur. Inom denna används specifikationerna för att reglera hur tillit etableras och upprätthålls till exempel hur metadata, nycklar och säkerhetskrav hanteras, hur ansvar fördelas och hur aktörer ansluts till federationen.

Inom federationsinfrastrukturen kan det finnas flera federationsområden med egna krav och regler, som baseras på infrastrukturens gemensamma grunder för interoperabilitet. På så sätt kan varje område anpassa lösningen efter sina behov men ändå vara en del av den nationella helheten.

### 3.3.1 Roller och ansvar

Roller inom infrastrukturen baseras på det förslag som Digg ger i sin slutredovisning<sup>13</sup>.

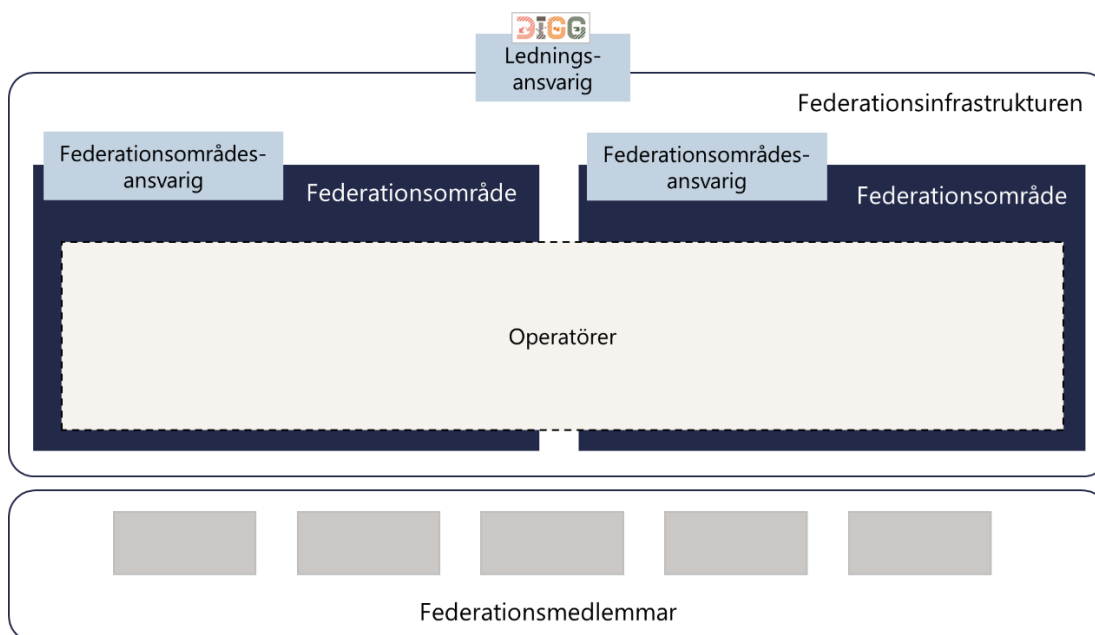
Digg föreslår att de blir **ledningsansvarig** aktör, som styr och reglerar den gemensamma federationsinfrastrukturen.

Inom infrastrukturen finns **federationsområdesansvariga** som ansvarar för ett eller flera federationsområden. Operatörer tillhandahåller federationsinfrastruktur tjänster som möjliggör att federationsmedlemmar kan anslutas och utbyta information med stöd av dessa federationsområden.

---

<sup>13</sup> Myndigheten för digital förvaltning *En sammanhållen infrastruktur för identitets- och behörighetshantering*. Dnr 2025-04363

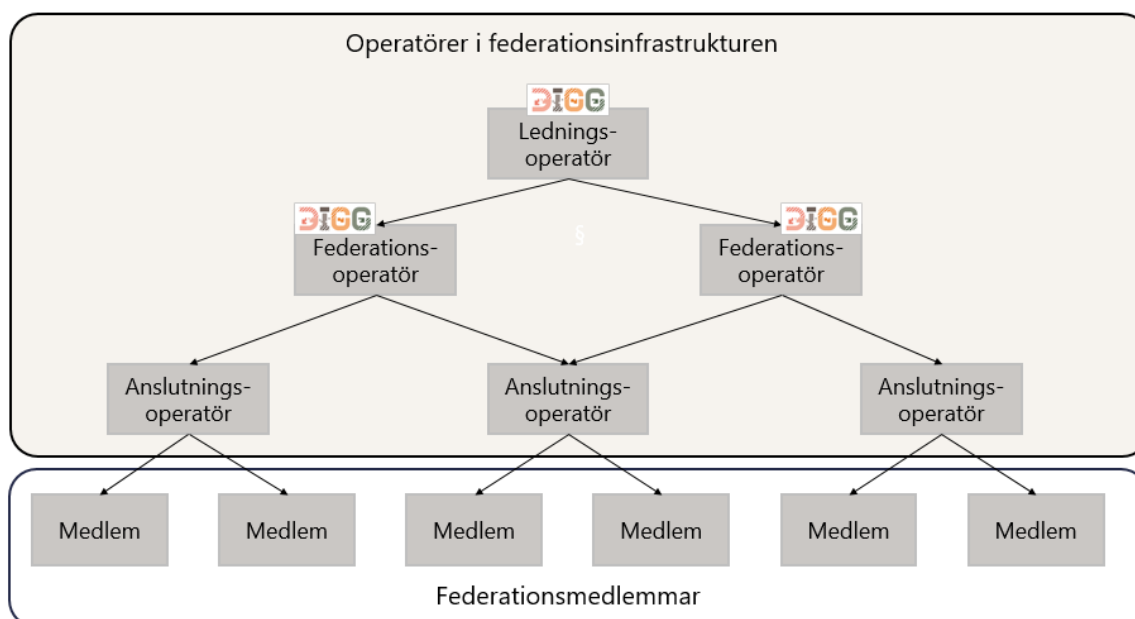
Figur 2. Roller i federationsinfrastrukturen



E-hälsomyndigheten gör bedömningen att myndigheten ska ta rollen som federationsområdesansvarig för ett federationsområde inom hälso- och sjukvård som åtminstone omfattar behov för EHDS, NDI och NLL. Se mer om tillämpning av infrastrukturen inom sektorn, inklusive vilka organisationer som föreslås ta olika roller, i kapitel 4 *Användning av infrastrukturen inom hälso- och sjukvård*.

För att infrastrukturen ska fungera i praktiken krävs även operativa tjänsteorienterade roller. Dessa roller innefattar olika typer av operatörer och är tekniskt inriktade.

Figur 3. Operatörsroller i federationsinfrastrukturen



**Ledningsoperatören** har det samlade operativa ansvaret för att samordna federationsinfrastrukturen som helhet. Rollen säkerställer att gemensamma principer, processer och tekniska ramverk tillämpas konsekvent och att infrastrukturen utvecklas på ett enhetligt och hållbart sätt. DigG kommer att vara ledningsoperatör.

Ledningsoperatören följer upp hur regler och villkor efterlevs, stödjer etablering av nya federationsområden och samverkar med de aktörer som ansvarar för teknisk drift inom sina respektive delar.

Uppdraget omfattar att, i samverkan med federationsområdesansvariga, federations- och anslutningsoperatörer, förvalta och vidareutveckla de gemensamma stödfunktioner som behövs för anslutning, incidenthantering, ändringshantering, samt att samordna kommunikation och vägledning för hela infrastrukturen.

Rollen fungerar därmed som den övergripande koordineringsfunktionen som håller ihop helheten – den som ser till att beslut, specifikationer och avtal omsätts i en fungerande och sammanhållen federationsinfrastruktur.

En **federationsoperatör** verkar inom ett eller flera federationsområden och ansvarar för hanteringen av federationsområdets tekniska struktur. Rollen säkerställer att de federationsinfrastrukturstjänster som tillhandahålls av anslutningsoperatörer samverkar enligt gemensamma standarder och specifikationer. DigG kommer att vara federationsoperatör.

Federationsoperatören svarar för aggregering, förmedling, publicering och validering av metadata, liksom för de processer som krävs för att bevara teknisk interoperabilitet och spårbarhet inom området. Rollen stödjer även etablering av nya anslutningsoperatörer genom att tillhandahålla tekniska gränssnitt, profileringar och vägledning för anslutning.

Rollen omfattar dessutom att samordna tekniska förändringar, hantera incidenter och säkerställa att infrastrukturen inom federationsområdet upprätthåller hög säkerhet, tillgänglighet och kvalitet. Genom nära samverkan med federationsområdesansvariga, anslutningsoperatörer och ledningsoperatören bidrar federationsoperatören till att helheten fungerar som en sammanhållen och tillförlitlig federationsinfrastruktur.

En **anslutningsoperatör** verkar inom ett eller flera federationsområden och ansvarar för att aktörer tekniskt ansluts till federationsinfrastrukturen på ett säkert och standardiserat sätt. Rollen utgör länken mellan de anslutna organisationerna och federationsområdets tekniska strukturer.

Anslutningsoperatören hanterar registrering, aggregering, förmedling, publicering och uppdatering av anslutna aktörers metadata, samt säkerställer att dessa uppfyller gällande krav på format. Rollen stödjer också aktörer vid anslutning genom teknisk rådgivning, verifiering av anslutningsunderlag och testning av interoperabilitet.

Rollen omfattar att upprätthålla en tillförlitlig och aktuell information över anslutna komponenter, hantera incidenter relaterade till anslutning och publicering samt bidra till kvalitetssäkring av infrastrukturen som helhet. Genom samverkan med federationsoperatörer och ledningsoperatören bidrar anslutningsoperatören till att den gemensamma federationsinfrastrukturen förblir tekniskt sammanhållen, verifierbar och robust över tid.

Operatörsrollerna samverkar genom de federationsinfrastruktur tjänster som de tillhandahåller. Dessa tjänster möjliggör säker och verifierbar kommunikation mellan aktörer och utgör grunden för hur infrastrukturen fungerar i praktiken.

### 3.3.2 Tillitsmärken och egenskapsintyg

Ett tillitsmärke visar att en teknisk komponent hos en organisation uppfyller de krav på säkerhet, regelbundenhet och förmåga som krävs inom federationsinfrastrukturen eller ett visst federationsområde för att kunna skapa, förmedla eller använda behörighetsgrundande information. Tillitsmärken kan även användas för att beskriva egenskaper hos en ansluten komponent.

Tillitsmärken används för att synliggöra regelefterlevnad och därmed möjliggöra tillit mellan anslutna parter. Detta är centralt i de fall då datadelning ska ske mellan system hos olika organisationer där den begärande parten ansvarar för användarnas behörighetstilldelning, till exempel i fallet då en vårdgivare hämtar data från Nationella läkemedelslistan.

Utgångspunkten är att tillitsmärken uppstår inom respektive federationsområde och regleras inte av den ledningsansvarige. Detta innebär att den federationsområdesansvarige ansvarar för att avgöra vilka tillitsmärken som är tillämpliga inom federationsområdet och tillse att nödvändiga efterlevnadskontroller för ett tillitsmärke kan genomföras.

Tillitsmärkesägaren ansvarar för att definiera, dokumentera och förvalta tillitsmärket och de tillitsskapande krav som är kopplade till tillitsmärket. I arbetet med att ta fram krav och efterlevnadskontroller för tillitsmärken är det viktigt att beakta de kostnader som uppstår hos anslutande organisationer.

I Samordnad identitet och behörighet används så kallade egenskapsintyg för att informera om egenskaper för de system som anslutits till infrastrukturen. Tillitsmärken kommer att registreras och förmedlas genom egenskapsintyg.

### 3.3.3 Infrastrukturen i ett konceptuellt tekniskt perspektiv

Federationsinfrastrukturen är till för att beskriva och förmedla information om komponenter som är anslutna. Detta sker genom metadata som gör det möjligt för anslutna medlemmar att tekniskt hitta varandra och avgöra om den uppfyller de krav som gäller för en viss samverkan.

När metadata publiceras i federationsinfrastrukturen enligt denna modell behöver man skilja mellan olika typer av metadata. Detta tydliggör både vilken information som beskriver en komponents tekniska funktioner och vilken information som förmedlar tillit och policy.

I federationsinfrastrukturen delas metadata in i två huvudtyper:

- **Tekniskt metadata:** Beskriver komponentens tekniska funktioner och gränssnitt, exempelvis adresser, kryptografiska nycklar och vilka protokoll som stöds. Den används för att säkerställa interoperabilitet och för att anslutna medlemmar tekniskt ska kunna kommunicera med varandra.
- **Beskrivande metadata:** Innehåller information om förmågor, policyer och tillit. Här kan krav, eller andra intyg, kopplas till en komponent, så att mottagare kan

avgöra om den uppfyller de regler och förutsättningar som krävs i en viss samverkan.

Den tekniska lösningen bygger på en distribuerad modell där dessa metadata kan publiceras på två sätt:

- **Egenpublicerat metadata:** Varje medlem publicerar signerat metadata om de komponenter som de själva ansvarar för.
- **Publicerat metadata om annan komponent:** Operatörer kan publicera signerat metadata som beskriver eller intygar en annan medlems komponent, till exempel att korrekt metadata publicerats och att vissa definierade krav uppfylls.

En grundläggande princip är att all metadata är digitalt signerad av den medlem som publicerar den. Därmed kan mottagande part verifiera att informationen verkligen kommer från rätt avsändare och att innehållet inte har manipulerats.

Federationsinfrastrukturen realiserar genom tre typer av funktioner:

- **Publicering:** Federationsmedlemmar och operatörer ansvarar för att publicera signerat metadata, både om sina egna komponenter och, där det är relevant, om andras komponenter.
- **Förmedling:** Metadata görs tillgänglig genom federationsinfrastrukturjänster som operatörerna ansvarar för, där informationen aggregeras och tillgängliggörs på ett enhetligt sätt.
- **Verifiering:** Medlemmar och operatörer kan, med hjälp av federationsinfrastrukturjänsterna, slå upp och kontrollera metadata för att säkerställa att den är korrekt och giltig.

Eftersom lösningen är distribuerad behövs ingen central katalog som alla måste uppdatera. I stället bygger helheten på att metadata kan publiceras av flera medlemmar och operatörer och hämtas dynamiskt vid behov. Federationsinfrastrukturjänsterna säkerställer att informationen kan förmedlas och verifieras på samma sätt oavsett vem som publicerat den.

Lösningen kombinerar tre egenskaper:

- **Decentralisering:** Medlemmar och operatörer ansvarar för metadata, men även andra kan bidra med kompletterande beskrivningar och intyganden.
- **Öppenhet:** Gemensamma format och öppna standarder gör att informationen kan delas och förstås av alla.

- **Verifierbarhet:** Infrastrukturen gör det möjligt att förmedla och kontrollera metadata så att den är äkta och användbar.

### 3.3.4 Teknisk realisering av infrastrukturen

Under 2025 har Digg driftsatt testmiljö, avseende federationsoperatörstjänster, som kan användas för tekniska verifieringar. Internetstiftelsen har också skapat testmiljö avseende tjänster i rollen som anslutningsoperatör. E-hälsomyndigheten har lanserat en extern testmiljö som erbjuder en anpassad åtkomstlösning för myndighetens tjänster.

Produktionssättning kan ske först då rättsliga förutsättningar finns. Givet att dessa förutsättningar finns på plats är E-hälsomyndighetens bedömning att teknisk realisering i produktionsmiljöer kan ske under 2026.

## 4 Användning av infrastrukturen inom hälso- och sjukvård

Detta kapitel beskriver hur infrastrukturen som realiseras genom Enas Samordnad identitet och behörighet kan komma att användas inom hälso- och sjukvården.

### 4.1 Hur förhåller sig infrastrukturen till dagens situation

Den föreslagna infrastrukturen adresserar och skapar förutsättningar för att lösa dagens problem med bristande interoperabilitet och tillit mellan aktörer, digitala tjänster och befintliga federationer, som till exempel mellan Sambu och HSA. Organisationer får möjlighet att efter godkännande av uppfyllda krav, ansluta till federationsinfrastrukturen och därefter samverka med andra aktörer och digitala tjänster både inom och mellan olika sektorer via federationsinfrastrukturen.

Ambitionen är att de samverkan- och tillitsstrukturer som redan är etablerade ska kunna återanvändas genom ett nära samarbete med Digg, Internetstiftelsen och Inera. I och med att framtagna krav har sitt ursprung i tillitsramverken för Sweden Connect, Sambu, HSA och SITHS så skapar det förutsättningar för att underlätta anslutningen för de i dessa federationer redan anslutna aktörerna.

## 4.2 Tillitstruktur för sektorns behov

Modellen för Samordnad identitet och behörighet bygger på att en federationsområdesansvarig finns för ett visst federationsområde. Inom ramen för området är det den federationsområdesansvariga som bland annat äger och ställer krav kopplade till eventuella tillitsmärken för samverkan inom området.

För bredare samverkan mellan olika federationsområden finns möjlighet att tekniskt registrera tillitsmärken hos federationsoperatören (Digg). Det behöver utredas vidare hur ansvarsförhållanden ska se ut i dessa fall, och på vilket sätt användningen behöver regleras mellan de olika samverkande federationsområdena.

E-hälsomyndigheten behöver, i sin roll som federationsområdesansvarig, inom ramen för de tillämpningar där federationsinfrastrukturen ska användas, såsom EHDS, NDI och NLL, ta ansvar för etablering av nödvändiga tillitsmärken samt efterlevnadskontroll av dessa. Detta är inget som den nationella sektorsöverskridande infrastrukturen tillhandahåller. E-hälsomyndigheten bedömer att ett eller flera generella tillitsmärken, som innefattar säkerhetsrelaterade krav, behöver etableras inom federationsområdet. Dessa tillitsmärken benämns generella eftersom de ska kunna användas för olika tillämpningar inom sektorn.

## 4.3 Identitet- och behörighetshantering i EHDS och andra nationella behov

EHDS-förordningen vid primäranvändning kommer att realiserars genom så kallade tillgångstjänster, dels för patienter, dels för hälso- och sjukvårdspersonal. Vidare ställer förordningen också krav på att de prioriterade kategorierna ska registreras i ett elektroniskt hälsodokumentationssystem (EHR-system).

Följaktligen kommer en överföring av hälsodokumentation från EHR-system till tillgångstjänst behöva kunna ske för att där användas på de sätt som förordningen stipulerar, exempelvis kunna uppvisas för patienter och hälso- och sjukvårdspersonal. För att möjliggöra denna informationsöverföring håller en nationell digital infrastruktur i hälso- och sjukvården på att etableras<sup>14</sup>. Denna infrastruktur är förutsättningskapande och syftar till att säkerställa att information kan lokaliseras och efterfrågas.

---

<sup>14</sup> Uppdrag om att genomföra en nationell digital infrastruktur i hälso- och sjukvården och förbereda för att Sverige ska genomföra förordningen om det europeiska hälsodataområdet (EHDS) rörande primäranvändning, S2024/02156 (delvis)

Även annan datadelning sker och kommer att ske på nationell nivå, men utanför EHDS-förordningen, exempelvis den datadelning som sker inom ramen för Sammanhållen vård- och omsorgsgivardokumentation, SVOD. Samma principer råder för denna datadelning och samma grundläggande förutsättning avseende nationell digital infrastruktur och de komponenter som ingår där gäller för denna datadelning. I resten av detta avsnitt använd EHDS som utgångspunkt, med de begrepp som används inom EHDS, men resonemanget gäller även annan nationell datadelning inom sektorn.

Både den faktiska överföringen av hälsodokumentation (mellan EHR-system och tillgångstjänst) och kommunikation med komponenter i den förutsättningsskapande nationella digitala infrastrukturen kräver tillit till behörighetsgrundande information. Enas Samordnad identitet och behörighet kommer användas för att möjliggöra och stödja båda dessa informationsutbyten.

Det informationsutbyte som EHDS avser, där det potentiellt finns många system där användare kan titta på information (EHR-system som är tillgångstjänster) och potentiellt många ställen där information finns (EHR-system som delar hälsodata), innebär att utbytet är multilateralt, det vill säga förhållandet är många-till-många. För att möjliggöra detta behöver identitet och behörighet hanteras på ett gemensamt sätt, vilket inom Ena kan åstadkommas genom att utforma och tillämpa tillitsmärken för detta ändamål. När information efterfrågas måste den omedelbart kunna tillhandahållas. Detta regelverk behövs för att säkerställa att förutsättningar för informationsutbyte är uppfyllda.

E-hälsomyndigheten bedömer att ett generellt tillitsmärke som etableras inom federationsområdet kommer att användas för att stödja det informationsutbyte som stipuleras av EHDS. Utöver detta generella tillitsmärke är myndighetens bedömning att ett eller flera specifika tillitsmärken för informationsutbyte enligt EHDS-förordningen behövs.

Att vara ansluten till Ena är i sig inte tillräckligt för att avgöra om ett informationsutbyte kan ske enligt EHDS eller ej. När en förfrågan om information kommer till ett EHR-system behöver man otvetydigt kunna avgöra att frågan kommer från ett system som har rätt att begära informationen, alltså en tillgångstjänst. För att detta ska vara skalbart behövs någon form av central hantering av denna information och myndighetens bedömning är att tillitsmärken är ett ändamålsenligt sätt att åstadkomma detta.

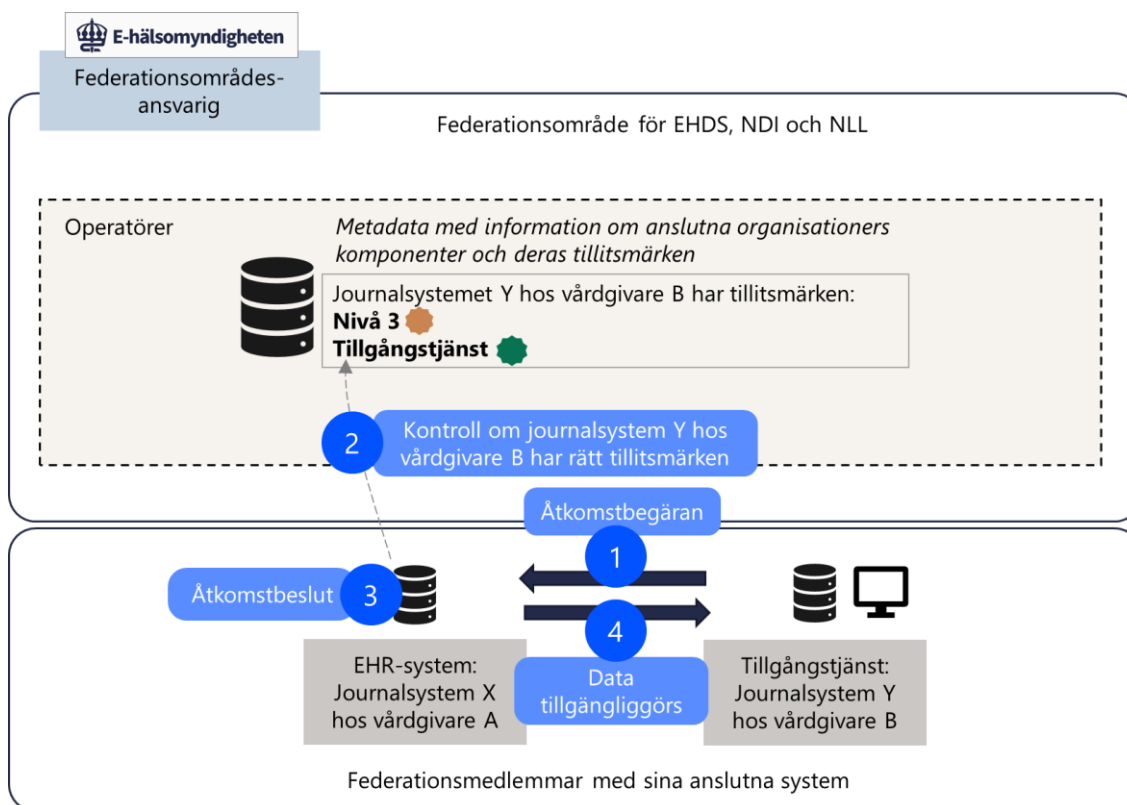
Vilka tillitsmärken som faktiskt behöver etableras för att möta kraven som EHDS-förordningen stället behöver analyseras vidare, men behovet av minst ett tillitsmärke som används för att signalera att ett system är av typen tillgångstjänst är redan nu tydligt. På liknande sätt behövs tillit till system hos vårdgivare som behöver åtkomst till E-hälsomyndighetens NDI-komponenter.

Tillitsmärkesägaren ansvarar för att definiera, dokumentera och förvalta tillitsmärken och de tillitsskapande krav som är kopplade till tillitsmärket. Rollen fokuserar på att säkerställa att det finns en tydlig och gemensam innebörd av varje tillitsmärke. Avseende det eller de tillitsmärken som blir aktuella för att möjliggöra EHDS gör myndigheten bedömningen att E-hälsomyndigheten är lämplig som tillitsmärkesägare.

Som en del i pågående arbete inom Enas Samordnad identitet och behörighet finns en ambition att Inera och Internetstiftelsen etablerar sig som anslutningsoperatörer. Det behöver utredas vidare om dessa operatörer kan anses vara tillräckligt för att samtliga organisationer som behöver dela hälsodata enligt EHDS har förutsättningar att göra det genom anslutning till Ena.

Eftersom E-hälsomyndigheten sannolikt kommer att tillhandahålla tjänster (tillgångstjänst) och komponenter, genom NDI, behöver E-hälsomyndigheten även ansluta som federationsmedlem. Det är nödvändigt för att nämnda tjänster och komponenter ska ingå i federationsinfrastrukturen och efterleva det regelverk som följer av EHDS.

Figur 4 Hur infrastrukturen skulle kunna användas för datadelning mellan vårdgivare



Figuren beskriver konceptuellt hur identitet- och behörighetsinfrastrukturen skulle kunna användas när ett journalssystem hos en vårdgivare (vårdgivare B) vill få åtkomst till hälsodata från en annan vårdgivare (vårdgivare A).

- 1) Vårdgivare B skickar en teknisk åtkomstbegäran till vårdgivare A. I denna åtkomstbegäran inkluderas behörighetsgrundande information.
- 2) Vårdgivare A kontrollerar, genom registrerat metadata i federationsinfrastrukturen, vilka tillitsmärken som vårdinformationssystemet Y hos vårdgivare B har.
- 3) Vårdgivare A tar åtkomstbeslut. Om systemet har rätt tillitsmärken, i detta exempel *Nivå 3* och *Tillgångstjänst*, kan den behörighetsgrundande informationen beaktas som underlag till åtkomstbeslutet. Åtkomstbeslutet baseras på ett i förväg fastställt regelverk.
- 4) Vårdgivare A ger åtkomst till hälsodata till vårdgivare B.

## 4.4 Nationella läkemedelslistan

E-hälsomyndighetens säkerhetslösning är utformad för att stärka skyddet av individens personliga integritet. Säkerhetslösningen ställer därför höga krav på de vård- och apoteksaktörer som ansluter till myndighetens tjänster. Syftet är att säkerställa identitets- och behörighetshanteringen, det vill säga att rätt person får åtkomst till rätt information.

Senast den 1 december 2025 ska alla vård- och apoteksaktörer vara anslutna till Nationella läkemedelslistan (NLL). När en aktör ansluter till NLL måste de använda E-hälsomyndighetens säkerhetslösning. I arbetet med anslutning till NLL har myndigheten fört dialog med aktörer som påverkas av detta krav. I dialog med regionerna och deras systemleverantörer lyftes ett antal utmaningar. Detta resulterade i att en kortsiktig säkerhetslösning utformades för att möta regionernas behov och introducerades som ett alternativ för regionerna under 2024. Detta har givit samtliga regioner förutsättningar att slutföra anpassningar och anslutning till NLL. Det finns samsyn mellan E-hälsomyndigheten och regionerna om att den kortsiktiga säkerhetslösningen är just kortsiktig och att en permanent lösning som bygger på arbetet inom Ena är en bra långsiktig lösning.

Myndigheten har jämte den kortsiktiga säkerhetslösningen sedan lång tid flera andra alternativ för anslutning som andra aktörer än regioner, som apotek, andra vårdgivare och veterinärer, kan nyttja. Bland dessa kan nämnas anslutning via identitets- och behörighetsfederationen Sambid och identitetsfederationen Sweden Connect. Myndigheten har fortsatt en långsiktig strategi för dessa alternativ. Anpassning av säkerhetslösningen mot Ena kommer att ske som ett tillägg jämte dessa befintliga alternativ. Det är följaktligen enbart den kortsiktiga säkerhetslösningen som på sikt kommer försvinna som alternativ.

E-hälsomyndigheten bedömer att ett generellt tillitsmärke som etableras inom federationsområdet kommer att användas när myndighetens säkerhetslösning anpassas till Enas Samordnad identitet och behörighet. Detta innebär att inga ytterligare tillitsmärken behöver utformas för att möta myndighetens behov av identitet och behörighet genom Ena som lösning.

I de befintliga alternativ som idag finns i myndighetens säkerhetslösning hanteras behörighetsgrundande information som beskriver exempelvis vilket yrke en användare innehar (exempelvis läkare). Denna information används i säkerhetslösningen för att avgöra vad en användare kan göra och vilken information en användare får tillgång till i NLL. Samma typ av hantering bedöms behövas när Samordnad identitet och behörighet ska användas i säkerhetslösningen.

Som ett led i myndighetens arbete inför anslutningar till NLL har även andra anpassningar gjorts för att ge aktörer med olika förutsättningar mer anpassade alternativ i säkerhetslösningen. Ett exempel på detta är det alternativ som benämns som användarorganisation med central behörighetshantering. Detta alternativ innebär att information om användarens identitet fortsatt förmedlas till myndighetens säkerhetslösning. Behörighetsgrundande information hanteras däremot genom uppslag i centrala källor, där Socialstyrelsens register över legitimerad hälso- och sjukvårdspersonal (HOSP) och Bolagsverkets tjänst Mina ombud används. Även i detta alternativ i säkerhetslösningen finns möjlighet att göra en anpassning till Samordnad identitet och behörighet, för att erbjuda detta som en möjlig väg att ansluta till E-hälsomyndighetens register och tjänster.

Sammantaget görs bedömningen att det finns goda möjligheter att anpassa myndighetens säkerhetslösning till Samordnad identitet och behörighet, och att detta kommer hantera de utmaningar som regionerna och deras systemleverantörer påpekade avseende myndighetens ordinarie säkerhetslösning. Det kommer dock kräva fortsatt utvecklingsarbete och det finns beroenden till att arbetet i Ena fortsätter med etablering av exempelvis operatörer för anslutning.

## 4.5 Roller i infrastrukturen

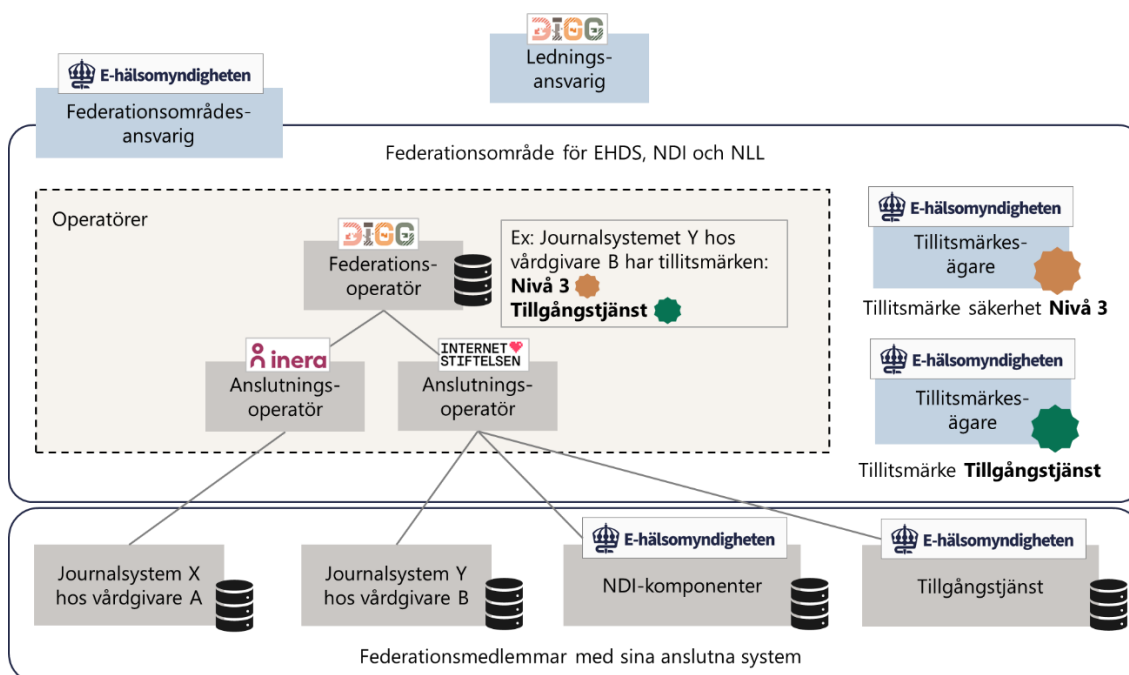
Digg föreslår att de blir ledningsansvarig för den nationella federationsinfrastrukturen samt roll som federationsoperatör.

E-hälsomyndigheten bedömer att myndigheten ska ta rollen som federationsområdesansvarig för ett federationsområde inom hälso- och sjukvård som åtminstone omfattar behov för delning av hälsodata enligt EHDS-förordningen, NDI och NLL. Vidare bedömer E-hälsomyndigheten att myndigheten ska vara tillitsmärkesägare för tillitsmärken som krävs för att tillämpa infrastrukturen för dessa behov.

Inera och Internetstiftelsen deltar i arbetet inom Samordnad identitet och behörighet och har idag till stora delar en roll inom HSA respektive Sambid som motsvarar det ansvar som anslutningsoperatörer kommer att ha. Det är önskvärt att fler aktörer tillkommer. E-hälsomyndigheten kommer, givet att E-hälsomyndigheten får fortsatt uppdrag att tillgängliggöra infrastrukturen, därför att arbeta för att främja tillkomst av operatörer för sektorns behov.

Följande bild visar ett exempel på hur det skulle kunna se ut, inklusive deltagande organisationer, om infrastrukturen tillämpas för delning av hälsodata för primäranvändning genom NDI.

Figur 5. Hur federationsinfrastrukturen skulle kunna se ut för delning av hälsodata genom NDI



## 4.6 Robusthet och tillgänglighet

Digitalisering och teknikutveckling skapar helt nya möjligheter i samhället, men också nya sårbarheter. Sverige är ett i hög grad digitaliserat land, vilket innebär att informations- och cybersäkerhet är viktigt för hela totalförsvaret och samhället. Digitala tillgångar ska inte kunna förstöras, manipuleras eller hamna i en angripares händer. Digitala tjänster för samhällsviktiga funktioner måste vara robusta och resilienta. Arbetet med informations- och cybersäkerhet samt digitalisering behöver gå hand i hand i syfte att skapa nödvändig säkerhet och robusthet i systemen. Detta samtidigt som de positiva effekterna av den fortsatta digitaliseringen av samhället möjliggörs.

Det kan finnas risker med att ha tillgänglighetskritiska tjänster och information samlad eller endast åtkomligt via en enda tjänst. Både tjänster och information skulle kunna utgöra mål för olika antagonisters angrepp. Konsekvenser av angrepp skulle kunna innebära störningar såväl gällande tillgänglighet, riktighet som konfidentialitet. Det är därför viktigt att de aktuella tjänsterna utvecklas för att hantera dessa risker.

För att säkerställa hälso- och sjukvårdens behov kommer systemen och tjänsterna i federationsinfrastrukturen att behöva vara robusta och tillgängliga. Exempelvis kommer tillgänglighetskritiska informationsmängder, såsom uppslags- och verifieringstjänster

vilka tillhandahåller metadata och medger kontroll av tillit, behöva tillhandahållas på ett distribuerat vis för att säkerställa informationstillgången. Dessutom kan det komma att behövas redundans i form av flera tillgängliga tjänsteleverantörer och operatörer. Utöver det robusta tillhandahållandet är det sannolikt lämpligt att metadata i många fall lagras lokalt, av prestandaskäl såväl som för att öka tillgängligheten ytterligare.

## 4.7 Rättsliga förutsättningar

Digg har i uppdrag att analysera behovet av och lämna förslag på författningsändringar som krävs för att utveckla en sammanhållen infrastruktur för identitets och behörighetshantering, som ska kunna tillhandahållas inom ramen för Ena. De rättsliga förutsättningarna för hur infrastrukturen ska kunna realiseras har därmed varit under utredning, vilket inneburit att E-hälsomyndighetens möjligheter att bedöma de rättsliga konsekvenser och eventuella behov för hälso- och sjukvårdssektorn varit begränsade.

Inom hälso- och sjukvårdssektorn finns det olika behov och krav avseende krav på identitet- och behörighetshantering. Nationella läkemedelslistans krav för behörighet följer av den reglering som finns för NLL, som utgår ifrån att vissa yrkeskategorier har rätt till viss information. Hälso- och sjukvårdspersonals behörighet i vårdssituationer till andra vårdgivares information om en patient följer av den behörighet som den vårdgivare som personalen arbetar för har satt. I de fall då det räcker med att endast kontrollera yrkeslegitimation för att ge åtkomst till uppgifter är det i många fall möjligt att kontrollera mot en central källa såsom HOSP. I de fall då behörigheten för hälso- och sjukvårdspersonalen styrs av den behörighet som vårdgivaren som personal arbetar för har satt, finns det ingen sådan nationell central källa som håller information om hur en vårdgivare har satt sin personals behörighet. Det krävs i det andra fallet därmed en tillit till att denna arbetsgivare har satt sina behörigheter på ett korrekt sätt.

För hälso- och sjukvårdssektorn så bygger eventuella tillitsramverk idag på frivillig anslutning och användning. En frivillig tillämpning av tillitsramverk kan resultera i att det finns aktörer som inte ansluter. Det behöver inom hälso- och sjukvårdssektorn utredas hur tillämpning av infrastrukturen och eventuella tillitsmärken fastställda av E-hälsomyndigheten kan användas för att kunna uppnå tillit mellan parterna.

Det rättsliga ramverket som Digg presenterar för identitets och behörighetskontroller omfattar inte eventuella aktörer som kommer att behöva fastställa eller utfärda ett tillitsmärke. Ramverket är dock tänkt att vara utformad på sådant sätt att de inte kommer att hindra de eventuella kompletteringar av infrastrukturen som kan behövas genom exempelvis introducering av tillitsmärken.

Rättsliga förutsättningar för tillämpning av identitets- och behörighetsinfrastrukturen för hälso- och sjukvårdssektorn har inte varit möjligt att utreda närmare förrän Digg presenterat sitt förslag. När förslaget från Digg nu finns presenterat, och det står klart att det kommer att behövas kompletteringar för att använda den för vissa tillämpningar inom hälso- och sjukvårdssektorn, behöver de rättsliga förutsättningarna för sådana kompletteringar utredas närmare. Det kan exempelvis krävas uppdrag genom författning till E-hälsomyndigheten att tillhandhålla tillitsmärken.

## 5 Överväganden och förslag

### 5.1 Tillgängliggöra HOSP och information om särskilda förordnanden

E-hälsomyndigheten föreslår att Socialstyrelsens register över legitimerad hälso- och sjukvårdspersonal och personal med bevis om rätt att använda yrkestiteln undersköterska (HOSP) ska tillgängliggöras till organisationer inom hälso- och sjukvården som har behov av att använda registret för behörighetstilldelning eller behörighetskontroller. Uppgifter i registret ska tillgängliggöras via API och e-tjänst.

E-hälsomyndigheten föreslår också att information om personer med särskilt förordnande tillgängliggörs på liknande sätt.

Socialstyrelsen ansvarar för att föra ett register över legitimerad hälso- och sjukvårdspersonal och personal med bevis om rätt att använda yrkestiteln undersköterska (HOSP)<sup>15</sup>. Uppgifterna används för upplysning om hälso- och sjukvårdspersonalens behörighet till arbetsgivare, apotek, myndigheter och allmänhet samt för tillsyn. Dessutom utgör registeruppgifterna underlag för statistik och prognoser över tillgången på hälso- och sjukvårdspersonal.<sup>16</sup>

Informationen i HOSP-registret är i flera fall behörighetsgrundande, exempelvis förskrivningsrätt för läkare. Det finns idag ett API för HOSP, men det är inte tillgängligt för bland annat privata vårdgivare. Kontroller möjliggörs istället exempelvis via ärenden som kräver manuell administrativ hantering. I de fall en organisation ska lämna ut data

<sup>15</sup> Förordning (2006:196) om register över legitimerad hälso- och sjukvårdspersonal och personal med bevis om rätt att använda yrkestiteln undersköterska

<sup>16</sup> Socialstyrelsen *Registret över legitimerad hälso- och sjukvårdspersonal och personal med bevis om rätt att använda yrkestiteln undersköterska (HOSP)*, <https://www.socialstyrelsen.se/statistik-och-data/register/halso-och-sjukvardspersonal/> [2025-12-03]

till en annan organisation, utan möjlighet till kontroll mot HOSP, måste den som ska lämna ut data kunna lita på den behörighetsgrundande informationen som följer med från begärande organisation. Dessa situationer kräver därmed tillit till den begärande organisationens behörighetsgrundande information. Behovet av denna tillit skulle inte behövas om utlämnande part själv hade tillgång till HOSP, eller andra källor med behörighetsstyrande attribut, och därmed kunde göra kontrollen innan utlämnandet.

I Socialstyrelsens remissvar<sup>17</sup> i SOU 2021:39 *Ombuds tillgång till vård- och omsorgsuppgifter och förenklad behörighetskontroll inom vården* ansåg myndigheten att möjligheten att kunna kontrollera en persons behörighet i HOSP genom sökfunktion på internet kan vara till stor nytta för arbetsgivare och myndigheter som behöver uppgifter om behörighet i sin verksamhet. Vidare ställde sig Socialstyrelsen positiv till utredningens förslag om att myndigheten får medge elektronisk tillgång genom direktåtkomst eller annat elektroniska utlämnande till offentlig- eller privat vårdgivare.

Det finns även möjlighet till särskilt förordnande för läkare<sup>18</sup>. Uppgifter om dessa förordnanden är inte en del av HOSP-registret eller digitalt tillgängliga för motsvarande kontroller som HOSP-registret. Dessa uppgifter behöver också finnas digitalt tillgängliga.

Sammantaget bedömer E-hälsomyndigheten att uppgifter i HOSP och uppgifter om särskilda förordnanden inte finns digitalt tillgängliga för de aktörer inom hälso- och sjukvårdssektorn som skulle ha nytta av den avseende behörighetstilldelning och behörighetskontroll. Detta leder istället till manuell administration och behov av tillit till behörighetsinformation från andra parter. Tillgängliggörande av dessa uppgifter skulle bidra till ökad säkerhet inom sektorn.

---

<sup>17</sup> Socialstyrelsen remissvar i SOU 2021:39 *Ombuds tillgång till vård- och omsorgsuppgifter och förenklad behörighetskontroll inom vården*

<sup>18</sup> HSLF-FS 2022:20 *Socialstyrelsens föreskrifter och allmänna råd om särskilt förordnande att utöva läkaryrket*

## 5.2 Rekommendation till fortsatt arbete

Arbetet med identitet- och behörighetsinfrastruktur inom Ena behöver fortsätta, med fokus på tillämpning, förvaltning och vidareutveckling av infrastrukturen.

E-hälsomyndigheten föreslår därför att myndigheten får i uppdrag att fortsatt tillgängliggöra infrastrukturen för användning inom hälso- och sjukvården, vilket förutsätter att myndigheten innehar rollen som federationsområdesansvarig. Uppdraget ska bland annat utreda de rättsliga förutsättningarna för att vara federationsområdesansvarig. Uppdraget behöver även ta fram vissa sektorsspecifika kompletteringar för delar som den sektorsöverskridande infrastrukturen inte tillhandahåller och utreda rättsliga förutsättningar för dessa kompletteringar. Uppdraget ska även stödja anslutande organisationer.

För att infrastrukturen ska kunna användas för olika typer av tillämpningar behöver operatörer etableras inom infrastrukturen. För att anslutande organisationer, såsom vårdgivare, ska kunna använda infrastrukturen för säker delning av hälsodata behöver dessa organisationer bli medlemmar och ansluta sina system.

Därför behövs ett fortsatt aktivt arbete inom Ena för att stödja blivande operatörer och federationsmedlemmar i deras arbete. Utöver anslutningsarbete behövs även fortsatt förvaltning och vidareutveckling av infrastrukturen inom ramen för Ena. E-hälsomyndigheten behöver ta ansvar för att stödja anslutande organisationer inom hälso- och sjukvården.

Infrastrukturen behöver kompletteras med vissa delar för att kunna användas inom hälso- och sjukvården. Dessa kompletteringar görs av den federationsområdesansvarige. E-hälsomyndigheten ser det som naturligt att myndigheten blir federationsområdesansvarig för ett federationsområde som åtminstone omfattar behov för delning av hälsodata enligt EHDS-förordningen, NDI och NLL. I rollen som federationsområdesansvarig ingår bland annat att ta fram tillitstruktur, etablera anslutningsoperatörer och ansluta federationsmedlemmar. När Digg har tagit fram en mer detaljerad beskrivning av rollen, kan E-hälsomyndigheten mer utförligt bedöma vad den innebär och utreda de rättsliga förutsättningarna för att ha rollen. E-hälsomyndigheten behöver även utreda rättsliga förutsättningar för att göra de kompletteringar som krävs för att infrastrukturen ska kunna användas inom hälso- och sjukvården.

E-hälsomyndigheten bedömer också att myndigheten ska vara tillitsmärkesägare för behov inom federationsområdet, ta fram krav på efterlevnadskontroller avseende tillitsmärken och tillse genomförandet av dessa kontroller.

## 6 Konsekvensanalys

### 6.1 Konsekvenser för hälso- och sjukvården

Infrastrukturen som beskrivs i denna rapport är i grunden frivillig att använda. För olika tillämpningar som vill använda infrastrukturen kan det dock bli aktuellt att göra anslutning till infrastrukturen obligatorisk. Konsekvensutredning behöver göras i de fall infrastrukturen görs obligatorisk att använda, vilket dock inte är en del av detta uppdrag. Det bör nämnas att E-hälsomyndigheten gör bedömningen att aktörer inom hälso- och sjukvården kommer att behöva ansluta till identitet- och behörighetsinfrastrukturen för realisering av NDI inklusive införandet av EHDS.

För en enskild organisation som, oavsett skäl, ska ansluta till infrastrukturen innebär det dock en påverkan. Vårdgivare behöver ha system som är anpassade till de tekniska specifikationer som tagits fram. De leverantörer som tillverkar och säljer vårdinformationssystem och IAM-system behöver därmed anpassa sina system till dessa specifikationer. Kostnader för utveckling och anpassning av system lär i många fall belasta vårdgivare.

De organisationer som ansluter sina system behöver uppfylla de tillitsskapande krav som ställs på till exempel informationssäkerhetsarbete. Förutsättningar hos olika organisationer skiljer sig åt i dessa avseenden. Exempelvis kan nämnas att vårdgivare som idag är anslutna till Sambi eller HSA troligtvis har relativt bra förutsättningar för att efterleva många tillitskrav.

Det är i dagsläget inte klarlagt hur prismodell för Samordnad identitet och behörighet kommer att se ut. Avgifter för anslutning och medlemskap i federationen kan därmed tillkomma.

### 6.2 Konsekvenser för individen

Individen påverkas inte direkt av denna infrastruktur. Uppdraget syftar bland annat till att öka patientsäkerhet och patienters integritetsskydd, samt förenkla delning av data mellan vårdgivare. Detta är till fördel för patienter. Samtidigt är det av yttersta vikt att infrastrukturen är säker, för att undvika patientsäkerhets- och patientintegritetsrisker.

## **6.3 Konsekvenser för E-hälsomyndigheten**

### **6.3.1 Fortsatt arbete med att tillgängliggöra infrastrukturen**

E-hälsomyndigheten föreslår i denna rapport att myndigheten fortsatt ska få fortsatt uppdrag att tillgängliggöra infrastrukturen inom hälso- och sjukvården. Fokus för fortsatt arbete kommer att ligga på frågor rörande bland annat sektorsspecifika kompletteringar, tillämpningar och anslutningsstöd. Bedömningen är att kostnaderna för detta arbete under 2026 uppgår till ca 10,6 miljoner kronor.

### **6.3.2 Användning inom nationell digital infrastruktur**

Resultatet av detta uppdrag innebär inte en direkt påverkan på E-hälsomyndigheten avseende tillämpning av infrastrukturen. Det är dock antagandet att infrastrukturen ska användas för den nationella digitala infrastrukturen i hälso- och sjukvården som E-hälsomyndighetens har i uppdrag att genomföra. Konsekvenser på E-hälsomyndigheten inom detta område bedöms inom det uppdraget.