Referensarkitektur för Telemedicin – del 1 – Ordinerad egenvård

Förutsättningar för ett nationellt skalbart och förvaltningsbart digitalt informationsutbyte

Bilaga till Referensarkitektur för vård och omsorg - T-boken

inera

inera

Revisionshistorik

Version	Datum	Författare	Kommentar
PA1	2018-02-14	Johan Eltes	Dokumentet skapat
PA2	2018-03-09	Johan Eltes	Inledning skriven samt behov och scenarier påbörjade
PA3	2018-03-15	Johan Eltes	Uppdaterat. Avsnitt 2 slutfört för första granskning. Utkast till styrande principer tillagt.
PA4	2018-09-05	Johan Eltes	Alla avsnitt utom Teknisk vy i första version för kommentarer i arkitekturrådet.
PA5	2018-09-06	Johan Eltes	Redaktionella förbättringar
PA6	2018-09-06	Johan Eltes	Redaktionella förbättringar efter presentation i arkitekturrådet
PA7	2018-09-07	Johan Eltes	Flyttat ut exemplen i informationssystemvyn till eget huvudavsnitt: ”Vägledning – Informationssystemvy” och skrivit om inledande i det avsnittet.
PA8	2018-09-10	Johan Eltes	Avsnittet Legal vy har utökats med skrivning om sammanhållen journalföring och särskilda krav rörande dataportabilitet.
PA9	2018-09-10	Johan Eltes	Beskrivningen av Formulärtjänsten är uppdaterad efter avstämning med tjänstens förvaltning.
PA10	2018-09-11	Johan Eltes	Beskrivningen av Uppsala-pilot och IBD-Home i avsnitt **Fel! Det går inrte att hitta någon**

			referenskälla. uppdaterade efter avstämning med en av leverantörerna bekom exemplen.
PA11	2018-09-11	Johan Eltes	Legal vy avstämd med juridiskt sakkunniga inom Inera. Text om flöde från eget utrymme till PDL-klassade komponenter har tagits bort, då det ändå inte ingår i denna version. Regel om märkning som medicinteknisk produkt har lagts till.
PA12	2018-09-17	Johan Eltes	Första utkast till säkerhetsvy.
PA13	2018-09-19	Johan Eltes	Informationssäkerhetsvyn utökad med krav rörande menprövning, samt att innebörden i flödespilarna förtydligats i figurerna i säkerhetsvyn.
PA14	2018-09-26	Johan Eltes	Informationssäkerhetsvyn uppdaterad med krav på autentisering i olika tekniska scenarion, vilket lett till beroende till ny utgåva av [IAM-RA].
PA15	2018-09-30	Johan Eltes	Infört korrektur från Anders Larsson och Jan Broman. Skrivit avsnittet Teknisk vy. Krav på följsamhet till [EUCODE] tillagt i specifika krav/infosäk.
Rev_A	2019-02-07	Stefan Gustavsson	Efter hantering av kommentarer från Arkitekturrådets medlemmar

Referenser och förkortningar

Id	Referens/dokument
T-boken	Styrande principer, vägledande exempel och teknisk referensarkitektur för vård och omsorg: http://rivta.se/documents/ARK_0019/
NordiskRA	”Towards a Nordic Reference Architecture for Personal Connected health and care Technology“: http://rivta.se/documents/ARK_0047/
SS2017	Socialstyrelsen, januari 2017, ”Hur arbetar hälso- och sjukvården med ”Egenvårdsinsatser - En kartläggning”, artikel nr 2017-1-27
Continua	Personal connected health alliance – Continua Design Guidelines: https://www.pchalliance.org/continua-design-guidelines
IndividVG	Utredning ”Enskilds Informationsutbyte med vårdgivare genom externa tjänster/appar”, version PA6, Inera AB.
IAM-RA	Referensarkitektur för identitet och åtkomst: http://rivta.se/documents/ARK_0046/
T-boken	Nationell teknisk referensarkitektur för vård och omsorg: http://rivta.se/documents/ARK_0019/
FHIR	Standarden HL7 FHIR: https://www.hl7.org/fhir/
RU-IndividVG	Rättslig utredning Enskilds informationsåtkomst
GDPR	Dataskyddsförordningen: https://www.datainspektionen.se/lagar-regler/dataskyddsforordningen/
Behovsbilaga	Nuläges- och behovsinventering genomförd inom ramen för arbetet med referensarkitekturen.
SaaS	E-Tjänst/System som tillhandahålls till juridiska och/eller fysiska personer i en gemensam installation i ett öppet nätverk – oftast internet. https://sv.wikipedia.org/wiki/Software_as_a_service.
EUCODE	Code of conduct for mhealth apps: https://ec.europa.eu/digital-single-market/en/news/code-conduct-privacy-mhealth-apps-has-been-finalised

1. Inledning

Detta dokument syftar till att komplettera den övergripande nationella referensarkitekturen för vård och omsorg [T-boken] med användningsfall relaterade till egenvård. Dokumentet beskriver tillkommande behov, målgrupper, principer och arkitekturer i förhållande till gällande version av T-boken. T-boken gäller i alla generella avseenden där inte annat anges. Dokumenten följer T-bokens uppställning.

Dokumentet är tänkt att tillämpas av regioner, landsting och kommuner för styrning av IT-relaterade egenskaper i samband med utveckling eller anskaffning inom området telemedicin. Denna version är avgränsad till delområdet ordinerad egenvård, även om flera av beståndsdelarna förutses ha en bredare tillämpbarhet– även utanför området Telemedicin.

1.1 Bakgrund

Begreppet telemedicin har en bred tillämpning. Det har historiskt omfattat distansutförande av aktiviteter med motsvarighet i fysiska besök så väl som utlokalisering av specialiserad vård. Men numera – särskilt inom egenvård och individbeslutad-monitorering – har begreppet börjat användas för tjänster som förutsätter digitalisering och där patienten själv är en nödvändig aktör. Alltså tjänster som aldrig har funnits eller erbjudits patienten som fysiska besök. Som exempel kan nämnas kontinuerligt algoritmiskt beslutsstöd som erbjuds den utskrivne patienten, där patienten föder algoritmen med egengenererade värden.

De nordiska länderna har samarbetat kring en teknisk referensarkitektur för ordinerad egenvård. Det var ett samverkansprojekt mellan nationella e-hälso-aktörer i Danmark, Finland, Norge och Sverige. Inera representerade Sverige. Deltagande länder publicerade resultatet [NordiskRA] i mars 2017. Arbetet omfattade även en bransch-dialog i deltagande länder. Branchorganisationen Swedish Medtech samordnade kommentarer från den svenska aktörer. Swedish Medtech uppmuntrade initiativet men menade samtidigt att det behöver följas av ett mer detaljerat arbete för att komma till praktisk nytta. Den svenska referensarkitekturen syftar till att nå en tillräcklig detaljeringsgrad.

Den nordiska referensarkitekturen omfattar standardisering av gränssnitt för information mellan systemkomponenter som kan ingå i en lösning för ordinerad egenvård. Målet har varit att verksamhetens behov av informationsutbyte ska kunna realiseras utan risk för oönskade leverantörsinlåsningar.

Den svenska anpassningen (detta dokument) har tagits fram av Sveriges regioner, landsting och kommuner under Ineras samordning och ledning. Den kompletterar den nordiska referensarkitekturen genom att dra nytta av möjligheter i befintlig nationell arkitektur, men ger också stöd för nya behov inom informationsutbyte och informationssäkerhet som inte rymdes i det nordiska arbetet.

Referensarkitekturen för telemedicin beskriver hur IT-stöd inom ordinerad egenvård kan organiseras för att uppnå prioriterade egenskaper och principer som beskrivs i avsnitt 4.

1.2 Avgränsningen till området Ordinerad egenvård

Området egenvård är stort och begreppet har i praktiken fått flera betydelser. Socialstyrelsen [SS2017] skriver följande om begreppet:

”Med begreppet egenvård avses enligt legaldefinitionen i egenvårdsföreskriften en hälso- och sjukvårdsåtgärd som legitimerad hälso- och sjukvårdspersonal bedömt att en patient själv kan utföra. Det går inte att säga generellt vilka åtgärder som utgör egenvård, utan det måste bedömas i varje enskilt fall. Egenvårdsinsatser enligt SOSFS 2009:6 kan därför innefatta allt från enklare åtgärder som exempelvis såromläggning och påtagning av stödstrumpor till mer avancerade åtgärder som hemdialys eller respiratorvård i hemmet. I kartläggningen har det framkommit att uttrycket egenvård står för två olika begrepp och att begreppet egenvård i den betydelse som avses i egenvårdsföreskriften skiljer sig från betydelsen i såväl allmänspråket som i fackspråket där egenvård ofta används för att beteckna en vårdåtgärd som en person själv vidtar, utan kontakt med hälso- och sjukvården.”

Denna version av referensarkitekturen är avgränsad till den egenvård som förskrivs av legitimerad hälso- och sjukvårdspersonal. Den ordinerade egenvårdens roll och användningen av digitalt stöd beskrivs utförligare i avsnitt 2.2.

1.3 Målgrupper

1.3.1 Befintliga målgrupper

Detta avsnitt fördjupar befintliga målgruppsbeskrivningar utgående från specifika behov inom telemedicin.

Arkitekturfunktioner nationellt, regionalt och lokalt

Regionala och nationella arkitekturfunktioner bidrar till att upphandlade och utvecklade lösningar inom ordinerad egenvård uppfyller krav avseende informationsutbyte, säkerhet, oönskade inlåsningseffekter, informationssäkerhet och följsamhet till nationella regelverk blir tillgodosedda. Genom en gemensam referensarkitektur för telemedicin kan arbetet nå en högre kvalité och ge stöd till mål som förutsätter samordnad kravställning.

Referensarkitekturen ska också ge stöd i portföljstyrningen. Med hjälp av referensarkitekturen ska arkitekter med strategiska och granskande uppdrag kunna värdera och positionera olika initiativ utgående från vilken påverkan initiativen har på samspelet mellan befintliga och planerade komponenter inom telemedicin:

- Rör det sig om ett initiativ inom egenvård – dvs ska referensarkitekturen tillämpas?
- Vilka av lösningens gränssnitt är strategiska att styra in mot överenskomna standarder?
- Vilka profiler/tjänstekontrakt av tillämpliga standarder behöver etableras och förvaltas?
- Är lösningen diagnos-specifik? Hur kan möjligheten att konsolidera till en framtida diagnosneutral egenvårdsplattform optimeras?
- Vilka krav bör ställas på befintligt vårdinformationssystem för att informationsflöden med egenvårdslösningar och vårdinformationssystemet ska kunna hanteras skalbart och ekonomiskt?

1.3.2 Nya målgrupper

Följande nya målgrupper har identifierats.

Leverantörer av egenvårdslösningar och deras kunder

Leverantörer av stödsystem för digitaliserad egenvård har behov av att förstå nationellt överenskomna principer för det digitala ekosystem deras system ska kunna verka i. Genom referensarkitekturen kan de planera för en nationell kundbas och därigenom nå snabbare och effektivare utrullning hos nya kunder. Det ligger förstås också i kundens intresse. Genom relationen till den nordiska referensarkitekturen förbättras förutsättningarna för att fler internationella produkter görs tillgängliga för den nordiska marknaden. Det leder i sin tur till att fler produkter blir tillgängliga för kunder på den svenska marknaden och att dessa produkter kan utbyta information med befintliga system.

Beställare av personlig medicinteknisk utrustning

Referensarkitekturen skapar förutsättningar för att nationellt enas om krav på personlig medicinteknisk utrustning (sensorer) som rör interoperabelt informationsutbyte med de IT-system och komponenter sensorerna ansluts till. Det kan i sin tur leda till att utbudet av interoperabla sensorer ökar.

2. Behov och scenarier

2.1 Arkitekturens intressenter

Inga nya intressenter har identifierats.

2.2 Scenariobeskrivningar

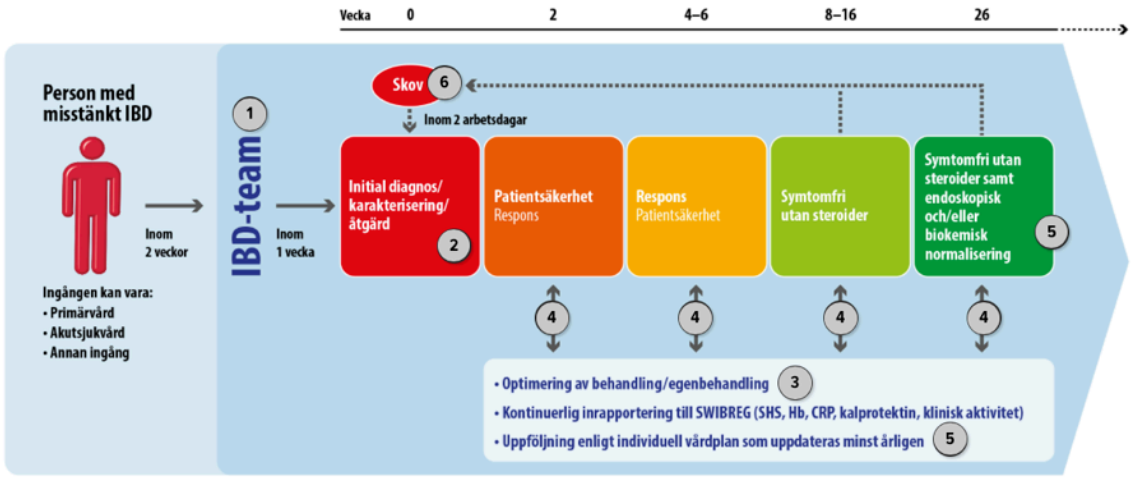
Scenariobeskrivningarna syftar till att lyfta fram kartlagda informationsutbytesbehov. Behoven som ligger till grund för scenariobeskrivningarna har inhämtats genom intervjuer med representanter för pågående initiativ inom ordinerad egenvård. Resultatet av intervjuerna redovisas mer ingående i behovsbilagan [Behovsbilaga].

Scenariobeskrivningarna tar sin utgångspunkt i behovsanalysens slutsatser men illustrerar dem genom att lyfta fram ett konkret exempel som spänner över samtliga identifierade informationsutbytesbehov: digitaliserat egenvårdsstöd i samband med ett verksamhetsutvecklingsprojekt inom inflammatorisk tarmsjukdom (IBD) inom Region Östergötland.

Projektets mål beskrivs enligt följande:

”I detta förbättringsprojekt vill vi implementera fyra nya konkreta arbetsverktyg i syfte att ställa om IBD-vården från traditionell resursoptimering till modern flödesoptimering och därmed öka tillgängligheten för patienten och sätta den individuella patientens behov i centrum. Målet är att uppnå bättre medicinska resultat och en tryggare och jämlik vård med oförändrad eller till och med minskad belastning/kostnad för sjukvårdsapparaten. Studier har visat att en stor andel av kostnaden för IBD-vården i Sverige är kopplad till akuta och oplanerade åtgärder vid skov av sjukdomarna. Ett centralt mål i projektet är att genom konsekvent monitorering av patienterna och ökad tillgänglighet förutse och förekomma akuta oplanerade åtgärder, vilket skulle vara kraftigt kostnadsbesparande. En avgörande komponent för att uppnå detta är att man lyfter in patienten själv i vårdteamet och utnyttjar patientens personliga resurser för att optimera omhändertagandet av sjukdomen. Förhoppningen är att det skall leda till större patientfokus med ökat medbestämmande för patienten samtidigt som vårdapparaten kan avlastas vissa insatser.”

Figur 1 illustrerar det verksamhetsmässiga sammanhanget för de egenvårdsinsatser som projektet bedriver med hjälp av digitalalt stöd:



Figur 1 Exempel på flöde för egenvårdsinsatser inom IBD

Figur 2 Flödesbeskrivning till föregående figur

Olika former av informationsutbyte mellan systemkomponenter förekommer eller planeras inom ramen för projektet. Följande behov har kunnat utläsas ur flödesbeskrivningen:

2.2.1 Vårdbegäran (1)

Här finns behov som relaterar till första linjens vård såsom själv-triagering, 1177 telefon/Video/chat-rådgivning, hitta och jämför vård (utbud) och patientens tidbokning. Dessa flöden ingår inte i den ordinerade egenvården och beskrivs därför inte ytterligare.

inera

2.2.2 Diagnostisering och förskrivning (2)

Kliniska beslut fattas och dokumenteras i journalsystemet, jämte beskrivningar av hälsotillstånd, ev. provsvar och andra beslutsunderlag. Här förskrivs också egenvård inom ramen för en vårdplan.

Delar av en strukturerad vårdplan (ordinerade egenvårdsaktiviteter) skulle med fördel kunna överföras från journalsystemet till egenvårdstjänsten, för där fler parametrar kan sättas enligt de möjligheter egenvårdslösningen erbjuder. Det kan t.ex. gälla att associera patienten med personlig medicinteknisk utrustning som ska användas i hemmet. I det aktuella fallet kan detta avse att associera egenvårdsplanen med den mobila enhet (mobiltelefon) som patienten kommer att använda tillsammans med appen vid avläsning av provstickor. Det kan också vara att precisera gränsvärden och frekvens för patientens inrapportering av mätvärden.

Det är oklart i vilken grad sådan information uppstår i strukturerad form i journalsystemet och därför också i vilken grad det finns risk för dubbelregistrering i samband med parametersättning av planerade egenvårdsaktiviteter.

Den aktuella lösningen bygger på en generell insamlingsinfrastruktur som samlar in och lagrar data i ett tillämpningsoberoende leverantörsnationellt datalager. Där finns också information om de monitoreringsbeställningar som sker från anslutna egenvårdslösningar. Den aktuella egenvårdslösningen skickar sådana beställningar till monitoreringstjänsten. Där kan appar som kopplats till monitoreringstjänsten hämta beställda monitoreringsaktiviteter och på så sätt anpassa interaktionen med patienten till sådan inmatning/datainsamling som är aktuell för de egenvårdsaktiviteter som ska rapporteras via appens formulär.

2.2.3 Professionens optimering (3)

Under pågående egenvårdsaktiviteter flödar information från patienten in till egenvårdslösningen. Information fångas av sensorer och formulär. Under detta flöde kan egenvårdslösningen påkalla ansvarig kontaktsköterskas uppmärksamhet. Det kan ske utgående från algoritmer som baseras på konfigurerade randvillkor för mätvärden, eller avvikelser i planerad rapporteringsfrekvens. Algoritmerna har också användning av information som fångats inom hälso- och sjukvården om den kan tillgängliggörs för egenvårdslösningen. Exempelvis kan en algoritm ha nytta av information om patientens besöksfrekvens på mottagningen.

Patienten kan också ta initiativ till kontakt med genom att starta en chat-dialog med kontaktsköterskan, boka en videokonsultation eller ringa. Kontaktsköterskan uppmärksammas genom epost eller personsökare. Vid behov av nya beslut kliniska engagerar kontaktsköterskan patientansvarig läkare (PAL). Det tycks saknas en professionsgemensam syn journalföring i samband med nya beslut. Det rör framför allt vilket urval av det strukturerade informationsunderlag som ska överföras som del av journalföringen. Det gäller såväl mätvärden som chat-historik och formulärsvar.

I ett annat exempel har en läkare uttryckt önskemål om att det medicinska beslutet författas i egenvårdslösningens gränssnitt, baserat på de underlag som finns där, men att själva journalposten som överförs till journalsystemet utgörs av en strukturerad sammanställning – inte de underliggande mätpunkterna i strukturerad form. I samband med Reumatologiskt beslutsstöd i Stockholms läns landsting, finns exempel på det omvända informationsutbytet: att läkaren

istället arbetar i journalsystemet, som i dokumentationssituationen hämtar in strukturerade underlag från beslutsstödsjournalen (här i rollen egenvårdslösning) och att sammanfattningen istället görs i journalsystemet.

I ett sådant scenario är egenvårdslösningen avgränsad till att enbart lagra och stödja den pågående egenvården. Det har dock framförts argument för att egenvårdslösningen är det IT-stöd där det bäst lämpar sig att peka ut vilka insamlade data som ska tillgängliggöras för journalsystemet inför journalföring av beslut, men att beslutet i sin helhet dokumenteras av användaren av journalsystemet. Detta synsätt var vid denna tidpunkt främst uttryckt i sammanhang med Ineras lösning för egenvård – Stöd- och behandlingsplattformen. Continua Design Guidelines [Continua] har också tagit fasta på det omvända flödet: att underlaget för journalföring som skapas i egenvårdslösningen förs över till journalsystemet på initiativ av egenvårdslösningen.

2.2.4 Patientens aktiviteter (4)

Under pågående egenvård är patienten användare av egenvårdslösningen. Patientens informationsutbyte rör inrapportering som relaterar till ordinerade egenvårdsaktiviteter. I det aktuella fallet handlar det om formulärbaserad inmatning via en app som är specialskriven för diagnosen i fråga. Appen kan via kameran översätta färgen på en provsticka till ett mätvärde patienten rapporterar in via formuläret.

Men det finns också generella kontaktvägar till sköterskan, såsom chat, video eller telefon som är öppna för patienten under egenvårdsperioden. I andra sammanhang kan sensorer, såsom blodtrycksmätare eller vågar, användas för automatiserad datainsamling till egenvårdslösningen. Överföringen kan då ske via patientens mobiltelefon eller via en insamlings- och kommunikationsenhet i hemmet. Det finns också exempel där sensorerna är inbyggda i personliga privata enheter så som smarta klockor eller i mobiltelefonen. I det aktuella fallet har appen för datainsamling en annan leverantör än den kombinerade egenvårds- och kvalitetsregisterlösningen. Därför har informationsutbyte behövt standardiseras dem emellan.

Dessutom har patienten ofta ett egenintresse i den strukturerade information som samlats in. Det gäller främst patienter med kroniska diagnoser (se forskning och publikationer kring s.k. Smart Patients, Sara Riggare m.fl.). Detta utgör dock inte alltid motiv för vårdgivaren att fortsatt behandla insamlade personuppgifter på individnivå. Den del av insamlad information som kommer att hanteras som journalinformation blir då möjlig att tillgängliggöra under minst de 10 år journalföringsplikten gäller.

Men eftersom all insamlad data gallras från egenvårdslösningen efter att behandlingen avslutats, kommer vårdgivaren därefter inte kunna tillgängliggöra annat än den del som journalförts. Patienten har förmodligen ett relativt omedelbart intresse i att erhålla en strukturerad kopia för hantering i egna IT-lösningar eller arkiv. Därför utgör gallringskravet på egenvårdsdata troligen inte en begränsning, så länge patienten erbjuds möjlighet till strukturerat utlämnande fram tills gallringstillfället. Gallringen bör då ske med viss tidsfördröjning så att patienten kan erbjudas ett tidsfönster som möjliggör ett ADB-utlämnande av all insamlad information.

2.2.5 Omprövning (5)

När patientens symptom tillfälligt försvunnit (remission), alternativt förvärrats, kan beslut leda till att egenvården avslutas, förändras eller pausas. Då uppstår samma behov av

informationsutbyte i samband med journalföring som beskrivits under punkt 3 – professionens optimering. I det aktuella exemplet förs också insamlade data kontinuerligt över till ett kvalitetsregister. I detta exempel är dock kvalitetsregistret en del i samma tekniska lösning, utan behov av informationsutbyte.

Generella informationsutbytesbehov mellan samverkande komponenter systematiseras och detaljeras i avsnitt 6. Avsnitt **Fel! Det går inrte att hitta någon referenskälla.** beskriver den tekniska lösningen för IBD Home i förhållande till referensarkitekturen.

3. Referensarkitekturen i ett sammanhang

Denna referensarkitektur är en komplettering av den gällande nationella referensarkitekturen för vård och omsorg [T-boken]. I den generella referensarkitekturen beskriver detta avsnitt hur arkitekturen ska tillämpas och förvaltas, samt vilken nytta den ska tillföra sina intressenter.

Eftersom Referensarkitekturen för telemedicin liksom T-boken är fokuserad på interoperabilitet och arkitektur vid informationsutbyte bör den hanteras på samma sätt.

4. Styrande principer

4.1 Vision utifrån befintliga behov

Behovet och intresset av att patienter ska kunna vårdas på distans är stort. Pågående initiativ inom regioner, landsting och kommuner bedrivs huvudsakligen i form av pilotprojekt. Pilotprojekten har i regel varit avgränsade till specifika diagnoser och utvalda patienter. IT-lösningarna är därför ofta valda med verksamhetsutveckling som enda kravställare. Förutsättningar för framgångsrik uppskalning och breddning har därför saknats. Det kan t.ex. gälla möjligheter att undvika dubbeldokumentation, eller – i de fall informationsutbyten alls förekommer med kringliggande IT-lösningar – att dessa har konstruerats utan inlåsningseffekter i förhållande till vald egenvårdslösning. Det är viktiga faktorer för att beakta när pilotaktiviteter skalas upp till inför breddinförande.

Referensarkitekturen syftar i första hand till att säkerställa icke-funktionella egenskaper – dvs egenskaper som har en indirekt påverkan på verksamheten, så som förändringsbarhet, ekonomisk livslängd, möjlighet att tillvarata innovationer på marknaden, möjlighet att integrera i ett nationellt, patientcentrerat perspektiv etc.

En referensarkitektur beskriver därför de IT-relaterade principer som är viktiga att vidmakthålla när ett nytt område utvecklas. Genom att följa principerna säkerställs en uppsättning prioriterade egenskaper i de lösningar som etableras. Dessa egenskaper som är viktig för systematisk tillämpning av egenvård tvärs patientgrupper och vårdverksamheter.

Analysen av genomförda intervjuer samt tidigare nordiskt arbete har lett fram till följande lista av prioriterade egenskaper. Listan är uppställd utan inbördes rangordning:

1. Dubbelregistrering behöver undvikas – isolerade egenvårdslösningar behöver integreras med övriga vårdinformationssystem
2. Förskriven personlig medicinteknisk utrustning (sensorer) behöver kunna delas mellan olika egenvårdsprogram oavsett vilken egenvårdslösning som används
3. De legala tolkningarna rörande dataskydd och informationsdelning behöver vara nationellt överenskomna för att ge en effektiv nationell marknad för egenvårdslösningar. Det ger också vårdgivare en trygghet inför breddinförande av nya innovativa lösningar på området.
4. Internationella standarder för informationsutbyte behöver tillämpas för att ge hälso- och sjukvården tillgång till ett internationellt utbud av egenvårdslösningar
5. De tekniska grundstrukturer som tillämpas behöver vara gemensamma med andra tillämpningsområden, såsom första linjens vård och digitala vårdmöten (video, formulär, chat) och kliniskt beslutsstöd (gemensam beslutsstödskomponent)
6. Strukturerad information som samlas in från individen ska där tillämpligt kunna bevaras och tillgängliggöras för kunskapsutveckling – oavsett om den journalförts som en del av den kliniska dokumentationen (mottagare är såväl individ som profession)
7. Arkitekturen ska stödja en gradvis (förutspådd) konsolidering av dagens diagnosbundna egenvårdslösningar till generella egenvårdsplattformar

I och med att användningen av digitala tjänster inom ordinerad egenvård ännu saknar större utbredning i svensk ehälsa saknas behov som relaterar till uppskalad användning. Det kan t.ex. gälla behov av "uthoppsintegrationer" med säker patientkontext och andra behov som är generella och kända i andra sammanhang inom ehälsa. Några av dessa behov tillgodoses genom att denna referensarkitektur baseras på mer generella, infrastrukturnära arbeten [IAM-RA] [IndividVG].

4.2 Principer

Referensarkitekturen ska ge vägledning till projekt och upphandlingar som delar dessa prioriteringar. Vägledningen ges i form av styrande principer för arkitektur men också genom att beskriva på vilket sätt principerna bör tillmötesgås – det vill säga enligt vilken arkitektur som lösningar inom ordinerad egenvård bör beställas och utvecklas. De styrande principerna och arkitekturbeskrivningarna i t-boken [T-boken] ger grundläggande vägledningen, men egenvårdsområdets särart samt ny lagstiftning (dataskyddsförordningen) leder till behov av att komplettera och detaljera såväl befintliga principer som mönster för arkitektur.

4.2.1 Precisering av befintliga styrande principer

Tabell 1 Precisering av befintliga styrande principer

Princip	Id	Specifika behov	Behovskälla	Styr mot egenskap
Informationssäkerhet	IT2	Konsekvenser av intrång i enskilda tjänster – särskilt externt förvaltade – ska minimeras med avseende på möjlighet att missbruka upprättade systemsamband.	T-boken	3
Nationell funktionell skalbarhet	IT3	Tillämpbar	T-boken	3
Lös koppling	IT4	Standardiserade gränssnitt är en förutsättning för ett skalbart ekosystem och för att minimera behovet av dubbelregistrering. Med anledning av den mognadsgrad och den ändamålsenlighet som	[T-boken] [NordiskRA]	1,2,3,4.5

		uppnåtts i internationell standardisering i förhållande till T-bokens referensarkitektur, ska utgångspunkten vara att tillämpa internationella standarder och i förkommande fall – internationell syftesanpassad profilering.		
Lokalt driven e-tjänsteförsörjning	IT5	I den mån lösningar för egenvård egenutvecklas av huvudmän enskilt eller genom Inera är denna princip tillämpbar.	T-boken	
Samverkan i federation	IT6	Patienten ska ha möjlighet att nå egenvårdstjänster via regionala eller nationella patientingångar utan att påtvingas förnyad autentisering. Det gäller även professionsanvändare.	T-boken	

4.2.2 Nya styrande principer

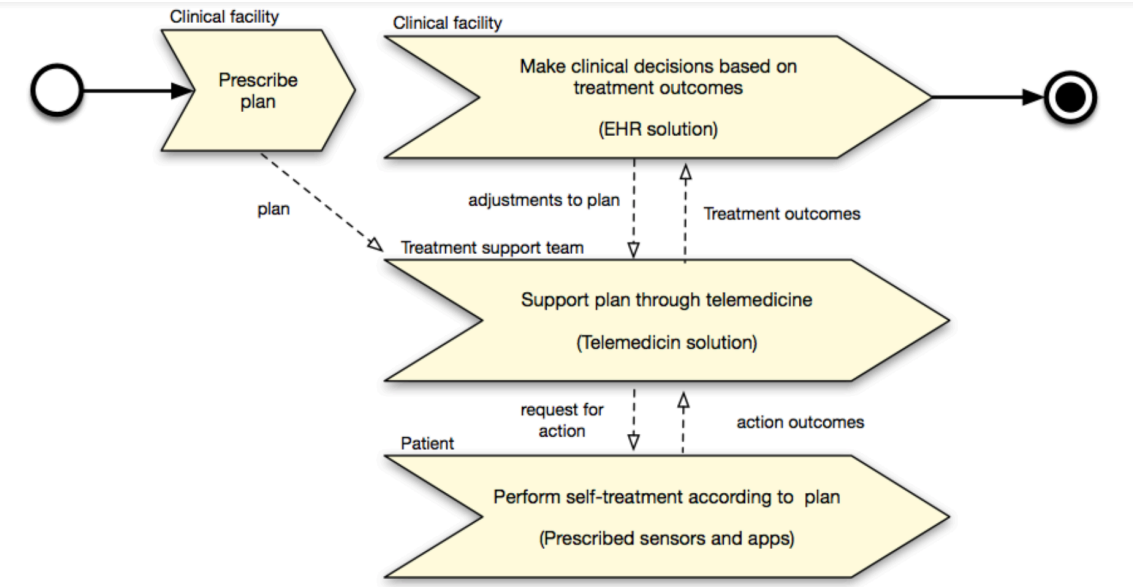
Tabell 2 Nya styrande principer

Princip	Id	Specifika behov	Behovskälla	Styr mot egenskap
Uppgiftsminimering	TM1	Personuppgifter minimeras i varje led. Patient-bindning av data görs så sent/nära journalsystemet som möjligt.	Dataskydds-förordningen	3

Lagringsminimering	TM2	Att personuppgifter som samlas in och hanteras i syfte ordinerad egenvård raderas efter att egenvården upphört.	Dataskydds-förordningen, Rättsutredning Enskilds informationsåtkomst[1]	3
Personuppgiftsansvar	TM3	Att all patientinmatad information hanteras och lagras inom ramen för personuppgiftsansvarig vårdgivare. Inom ordinerad egenvård saknas möjlighet för vårdgivare att tillhandahålla ett vårdgivarneutralt eget utrymme. Att utlämnande av registrerade personuppgifter till patientens eget utrymme i egen tjänst/app sker på ett sätt att personuppgiftsansvaret entydigt kan avgöras vid varje steg i informationsutbytet.	Dataskydds-förordningen, Rättsutredning Enskilds informationsåtkomst[2]	3
Dataportabilitet	TM4	Att all information inmatad av patienten blir tillgänglig för digitalt, portabelt utlämnande till patientens eget IT-stöd. Principen bör tillämpas trots att skyldighet inte föreligger inom PDL.	Avsnitt 2.2	7

5. Verksamhetsvy

Figuren nedan illustrerar referensarkitekturens omfattning utifrån olika intressentperspektiv och de behov den ska möta. Figuren är hämtad ur den nordiska referensarkitekturen. Den sammanfattar de informationsutbytesbehov som identifierats i behovsanalysen och som lyfts fram i scenariobeskrivningarna.



Figur 3 Intressenter och informationsutbyten i samband med förskriven egenvård enligt nordiska referensarkitekturen [NordiskRA]

Egenvårdsverksamheten bedrivs dessutom i ett sammanhang av andra intressenter så som kvalitetsregister och beslutsstödsjournaler. De behoven är hanterade i den generella referensarkitekturen (T-boken).

6. Informationssystemvy

Den nordiska referensarkitekturen [NordiskRA] definierar funktionella beståndsdelar i ett sådant IT-stöd. Dessa beståndsdelar – eller byggblock – används i följande avsnitt för att beskriva olika aspekter av arkitekturen – så som informationssäkerhet, lagrum, interoperabilitet, ansvarsområden, standardisering och möjliga logiska lösningsarkitekturer.

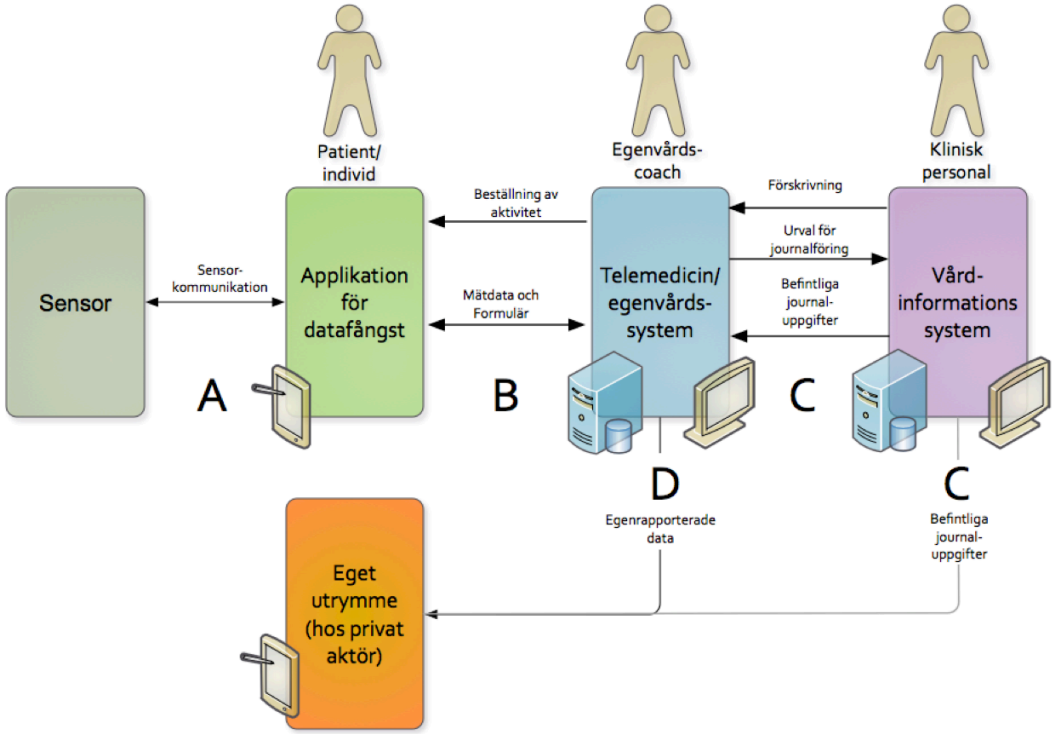
Beskrivningen av byggblocken blir på så sätt en gemensam begreppsapparat för att kommunicera arkitektur inom området telemedicin – en begreppsapparat som kan vara gemensam för de länder som deltagit i arbetet med den nordiska referensarkitekturen [NordiskRA].

Informationssystemvyn berör inte användningen av infrastrukturkomponenter så som tjänsteplattformar eller säkerhetstjänster. Dessa aspekter behandlas i avsnitt 10

6.1 Arkitekturens byggblock

Det är nödvändigt att sätta sig in i den funktionella uppdelningen mellan byggblocken för att kunna tillämpa referensarkitekturen.

Figuren nedan illustrerar byggblocken och deras ömsesidiga behov av informationsutbyte. Byggblocken är av logisk natur. De representerar funktionella områden som är möjliga att realisera som enskilda system men också som inbyggda funktioner i större -mer heltäckande systemlösningar. Dagens marknad för systemlösningar inom telemedicin och vårdinformationssystem erbjuder lösningar som är realiserade enligt den logiska uppdelningen. De vanligast förekommande lösningarna realiserar dock fler än ett byggblock i ett och samma mjukvarusystem. Men även det omvända förekommer – att ett byggblock är uppdelat i flera lösningar som exekverar på olika enheter.



Figur 4 Byggblock för arkitektur inom ordinerad egenvård

När ett eller flera av byggblocken är uppdelade i mer än ett system uppstår behov av att utbyta information på det sätt som pilarna indikerar. För- och nackdelar med olika konfigurationer av byggblock i form av vårdinformationssystem diskuteras i senare avsnitt. Här beskrivs byggblocken som om de realiserats som fristående systemkomponenter med behov av att utbyta information på ett standardiserat sätt.

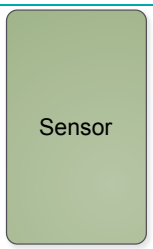
Arkitekturen saknar byggblock för beslutsstöd. Under arbetet har idéer uppkommit om att det skulle vara av värde att generella beslutsstödmoduler skulle kunna integreras i såväl vårdinformationssystem som i telemedicin/egenvårdsystem. Det vore som alternativ till dagens situation där telemedicin/egenvårdsystem i regel har inbyggt beslutsstöd.

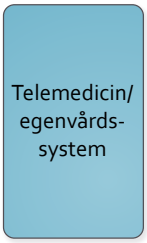
6.2 Funktionella byggblock

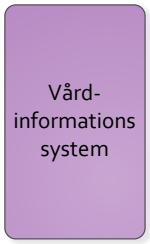
Tabell 3 beskriver byggblockens funktionella avgränsning.

Tabell 3 Funktionella byggblock

Byggblock	Beskrivning	Exempel
Sensor	En personlig enhet för automatiserad upptagning av fysiska mätvärden. I detta	Glukosmätare, blodtrycksmätare, våg,

	sammanhang är det underförstått att enheten hanteras i privat miljö av den person som är källan för uppmätta värden. En sensor kan vara en fristående enhet eller inbyggd i den enhet som exekverar en Applikation för datafångst (t.ex. en sensor i en smart klocka). En fristående sensor kommunicerar infångad mätdata med en enhet som har en *Applikation för datafångst*.	pulsmätare i en smart klocka
Applikation för datafångst 	Programvara på en enhet som tar emot mätvärden från en sensor eller möjliggör för patienten att manuellt mata in värden – t.ex. via ett formulär-gränssnitt. Programvaran kan vara fördelad över flera enheter – t.ex. en användargränssnittsdel i patientens mobila enhet och en s.k. ”back-end” i infrastruktur-operatörens driftsmiljö. Programvaran tar emot monitorerings- och/eller formuläruppdrag från ett Telemedicin/Egenvårds-system. Inhämtade formulär- eller sensordata förs över till ett Telemedicin/Egenvårds-system. Byggblocket har i regel bara användargränssnitt för patienten. Om byggblocket har en back-end kan användargränssnitt för profession förekomma – särskilt i de fall monitorerings- eller formuläruppdrag behöver konfigureras manuellt.	• Applikationer i en mobil enhet i hemmet som tar emot indata från uppkopplade sensorer och för över för lagring och ytterligare bearbetning i ”back-end”-funktioner i leverantörens datacenter. • Applikationer i en smart klocka som behandlar, lagrar och vidareförmedlar data från klockans inbyggda pulsmätare • En mobil applikation som med hjälp av kameran översätter provstickans färg (IBD) till ett mätvärde • En web-formulär-applikation (”front-end” + ”back-end”) för inmatning av vitalparametrar för överföring till Ineras Stöd- och behandlingsplattform

		• En generell formulärtjänst för patienter
Telemedicin/ Egenvårdssystem 	Ett informationssystem eller modul för ordinerad egenvård. Byggblocket består av funktionalitet för att… • definiera, initiera, styra och avsluta datainsamling utgående från en strukturerad behandlingsplan med ingående egenvårdsaktiviteter • strukturerade behandlingsplaner med ingående egenvårdsaktiviteter kan tas emot från vårdinformations-system eller konfigureras manuellt via användargränssnitt • tillämpa algoritmer för utvärdering av insamlad data (insamlad av individen och professionen) i syfte att dynamiskt anpassa egenvården enligt evidensbaserade metoder • aktivera digitala kontaktvägar mellan patient och profession • möjliggöra sammanfattning och överföring av kliniska slutsatser för journalföring • möjliggöra ADB-utlämnande av uppgifter insamlade från patienten till Eget utrymme i patientens egna tjänster Byggblocket har i regel användargränssnitt för både profession och patient. Insamlade patientuppgifter lagras tills behandlingsplanen är	• En moln-baserad (Software-as-a-Service) tjänst för ordinerad egenvård med stöd för en eller flera kroniska diagnoser • Ineras plattform för stöd- och behandling

	slutförd och journalförd i vårdinformationssystemet.	
Vårdinformations-system 	Ett informationssystem för att fatta och dokumentera kliniska beslut med tillhörande strukturerade beslutsunderlag så som mätvärden, remisser och labbsvar. Byggblocket kan… • ta emot och journalföra strukturerade sammanfattningar av egenvårdsutfall från Telemedicin/Egenvårds-system • möjliggöra ADB-utlämnande av strukturerade observationer/mätdata till patienten för lagring/hantering i Eget utrymme • förskriva och överföra ordinerad egenvårdsplaner till Telemedicin/ Egenvårdssystem	• Regionala och kommunala vårdinformations-system • Journalsystem som tillgängliggörs som molntjänst (”Software-as-a-Service”)
Eget utrymme 	Ett säkert digitalt utrymme för Personuppgifter – i form av session eller lagringsutrymme - där den enskilde förfogar över personuppgifterna och självständigt styr över vilka personuppgifter som hanteras. Den enskilde styr också självständigt hur och med vem personuppgifterna i det egna utrymmet delas med andra personuppgiftsansvariga eller enskilda Eget utrymme är en del-funktionalitet i en tjänst eller applikation som patienten använder baserat på eget beslut och som tillhandahålls av tredje part [IndividVG].	• En app i en mobil enhet som möjliggör överföring och lagring av strukturerad vårddokumentation från vårdinformationssystem och telemedicin-lösningar till en lagringsplats i den mobila enheten • En molntjänst riktad till specifika diabetiker, som möjliggör automatiserad överföring av labbvärden från vårdgivares journalsystem.

	Applikationen möjliggör för individen/patienten att ta emot, lagra och bearbeta individens inrapporterade mätvärden från Telemedicin/ Egenvårdssystem såväl som strukturerad information från patientens journal i olika vårdinformationssystem.	• En tjänst som ett läkemedelsföretag erbjuder Varan-patienter för att ge AI-baserade råd utifrån ordinationsuppgifter från patientens vårdgivare och egna puls- och blodtrycksmätningar

6.3 Informationsgränssnitt

De funktionella byggblocken har behov av att utbyta information. Dessa behov symboliseras av pilarna i Figur 4. Pilarnas riktning anger flödesriktningen. Pilarna ska alltså inte ses som API-anrop[3].

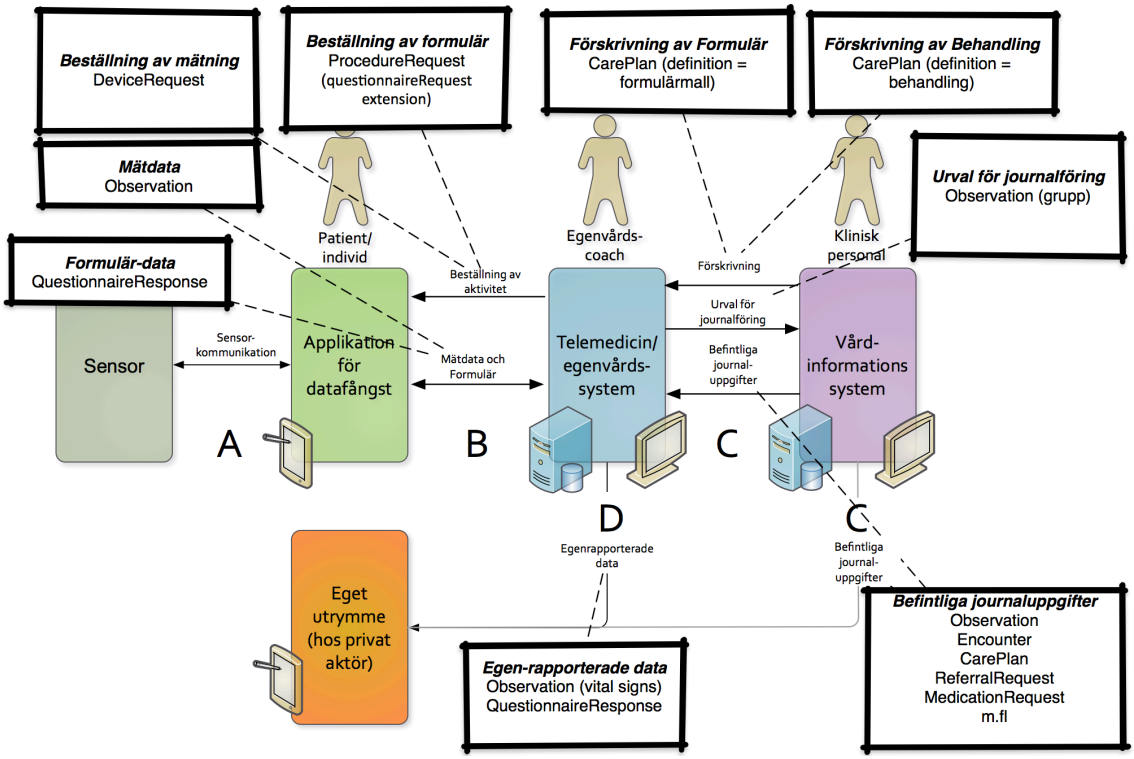
Dessa beskrivs i Tabell 4. Om en lösning saknar stöd för ett informationsutbyte uppstår krav på dubbelregistrering. Om en lösning har stöd för ett informationsutbyte, men på ett sätt som inte följer principen om lös koppling (IT4), uppstår risk för leverantörsinlåsning och förhöjda anskaffnings- och förvaltningskostnader.

Tabellen nedan beskriver de informationsgränssnitt som möjliggör automatiserade och standardiserade informationsutbyten mellan lösningar som stödjer arkitekturens byggblock.

Uppställningen delar in informationsgränssnitten i områden och användningsfall. Ett område består av de användningsfall för informationsutbyte som ingår mellan två byggblock i huvudflödet.

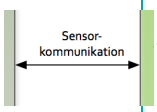
Användningsfallen beskrivs övergripande – både funktionellt och informatiskt. En del av den informatiska beskrivningen exemplifieras av referenser till representativa informationsstrukturer (”resurser”) ur standarden HL7 FHIR [FHIR]. Referenserna till FHIR illustreras i Figur 5.

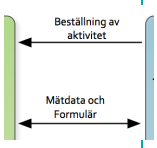
[3] Realiseringen i form av API:er kan ske enligt olika interaktionstyper, så som ”push” eller ”notifering + pull”. Valet av interaktionstyp påverkar vilken part som är tjänstekonsument respektive tjänsteproducent för det API som används. Men flödesriktningen är fortfarande densamma. Exakt vilken interaktionstyp som används för olika informationsgränssnitt preciseras av respektive profiler/tjänstekontrakt.

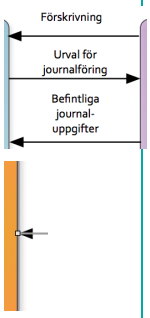


Figur 5 Användningsfall för informationsutbyte - FHIR

Tabell 4 Gränssnitt för informationsutbyte

Område	Användnings fall	Beskrivning	Exempel på standarder
A 	Sensor-kommunika-tion	Kommunikations-gränssnitt för datautbyte mellan sensorer och applikationer för datafångst.	ISO/IEEE 11073-104XX

B 	Beställning av aktivitet	Informationsutbyte som syftar till att ett telemedicin/egenvårdssystem ska kunna delge en applikation för datafångst parametrar som beskriver ett uppdrag att fånga data. Det kan gälla såväl formulär- som sensor-baserad datainsamling. Uppdraget kan till exempel omfatta information om *individ, mätningsfrekvens, sensor eller formulärmall, tidsrymd, vårdgivare och vilket telemedicin/egenvårds-system som ska ta emot insamlad data*.	FHIR DeviceRequest, FHIR ProcedureRequest med utökningen Questionnaire Request
	Mätdata och formulär	Informationsutbyte som syftar till att en applikation för datafångst ska förmedla resultatet av datafångsten till ett telemedicin/ egenvårdssystem. Informationen kan bestå av *mätdata eller formulärdata*. Det finns ett överlapp mellan dessa informationsmängder eftersom formulär-data kan vara mätdata. Vilken struktur som används beror av applikationsspecifika omständigheter. Men om mätvärdena har upphämtats av en sensor ska de överföras som mätdata.	FHIR Observation, FHIR Questionnaire Response

		Applikationen för datafångst skickar formulär/data till det Telemedicin/ egenvårdssystem som angivits i Beställningen av aktiviteten.	
C 	Förskrivning	Informationsutbyte som syftar till att ett vårdinformationssystem ska delge ett telemedicin/ egenvårdssystem en strukturerad plan över ordinerad egenvård. Planen beskriver vilka *egenvårdsaktiviteter* som ska utföras. Informationen i planen möjliggör för telemedicinsystemet att ge önskat digitalt stöd åt patientens egenvårdsaktiviteter. I sin enklaste form består planen av en referens till en *vårdplan-mall* som vårdpersonal manuellt har definierat i telemedicin/ egenvårdssystemet. Användningsfallet att ge vårdinformationssystemet tillgång till tillgängliga mallar i telemedicinsystemet är avgränsat från referensarkitekturen. En annan form av enkel plan är att begära in en fristående självskattning. I det fallet refererar planen en *formulärmall*.	FHIR *CarePlan* med referens till behandlingsdefinition eller formulärmall. För behandlingsdefinition: CarePlan.basedOn(PlanDefinition). För formulärbegäran: CarePlan.basedOn(Questionnaire).

		Planen ska också ange i vilket vårdinformationssystem som är mottagare av Urval för journalföring.	
	Urval för journalföring	Informationsutbyte som syftar till att överföra kliniskt beslutsunderlag från telemedicin/ egenvårdssystemet för journalföring i vårdinformationssystemet. Därigenom kan dubbeldokumentation undvikas. Informationen kan vara utvalda observationer med ursprung i insamlade mätvärden eller ifyllda formulär (självskattningar). Det kan också vara sammanfattningar av text (chat)- eller video-baserade dialoger mellan coach och patient som underlag för beslut om förändringar i förskrivningen (så som att avsluta egenvården). Informationen förs över till det Vårdinformationssystem som angivits om mottagare i Förskrivningen.	FHIR Observation. Observation.basedOn(CarePlan): Referens till CarePlan från förskrivning. FHIR Observation.related([Observation | QuestionnaireResponse]*): Lista av de formulärsvar och observationer som är del av denna sammanfattande observation.
	Befintliga journal-uppgifter till telemedicin-systemet	Informationsutbyte som syftar till att ge telemedicin/ egenvårdssystemet tillgång till strukturerad data över patientens vårdhistorik. Det kan t.ex. tillgodose behovet av historik data hos telemedicin/	FHIR Observation, FHIR Encounter, FHIR CarePlan, FHIR Medication Request, FHIR Condition m.fl.

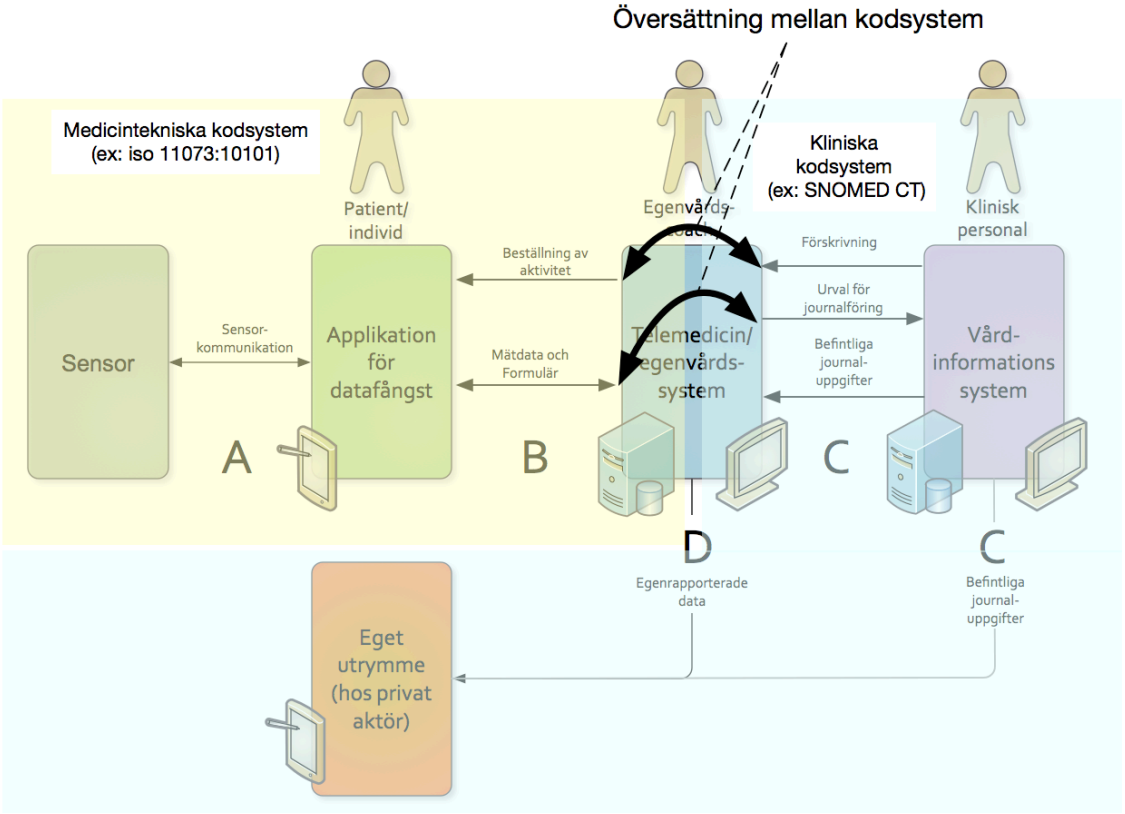
		egenvårdssystemets algoritmer för automatisk anpassning av egenvårdsaktiviteter: observationer, diagnoser, genomförda vårdplaner, läkemedelsordinationer, vård- och omsorgskontakter. Informationen kan vara avgränsad till den vårdgivare som ordinerat egenvården. Om telemedicin/ egenvårdssystemet uppfyller kraven på konsumtion av information inom sammanhållen journalföring [PDL] kan en mer komplett historik tillhandahållas. Man måste då också beakta begränsningar i möjligheten att lagra överförd information under egenvårdsförloppet, som kan gälla för direktåtkomst inom sammanhållen journalföring.	
	Befintliga journal-uppgifter till Eget utrymme Detta informations-utbyte är inte specifikt för telemedicin. Det redovisas här för att - tillsammans med område D	Informationsutbyte som syftar till ADB-utlämnande av strukturerad vårddokumentation till patientens egna utrymmen. Det kan t.ex. vara läkemedelsordinationer och behandlingar, observationer/ mätvärden, undersökningsresultat,	HL7 förvaltar profiler i detta syfte för följande FHIR-resurser. Profilerna används bl.a. av Apple Healthrecord: FHIR Medication Statement FHIR Medication Request FHIR Observation FHIR Diagnostic Report FHIR Immunization

	- ge ett komplett scenario för utlämnande till eget utrymme	vaccinationer och vårdplaner.	FHIR CarePlan
D 	Egenrapporterade data	Informationsutbyte som syftar till att ge patienten tillgång till de strukturerade uppgifter som samlats in från patienten som del av egenvårdsplanen. Det avser de data som patienten rapporterat genom gränssnittet ”Mätdata och formulär”.	FHIR Observation, FHIR Questionnaire Response

6.4 Kodsystem

Sensormarknaden tillämpar kodsystem för medicinteknisk utrustning. Continua Design Guidelines [Continua] profiler standardiserar på användning av medicintekniska kodsystem i A- och B-gränssnitten, samt rekommenderar kliniska kodsystem (så som SNOMED CT) för C-gränssnitten. Referensarkitekturen baseras därför på samma uppdelning. En konsekvens blir att Telemedicin/egenvårdssystemet behöver kunna översätta mellan tillämpade medicintekniska kodsystem och kliniska kodsystem.

Continua design guidelines [Continua] roll i referensarkitekturen beskrivs i avsnitt 6.6.



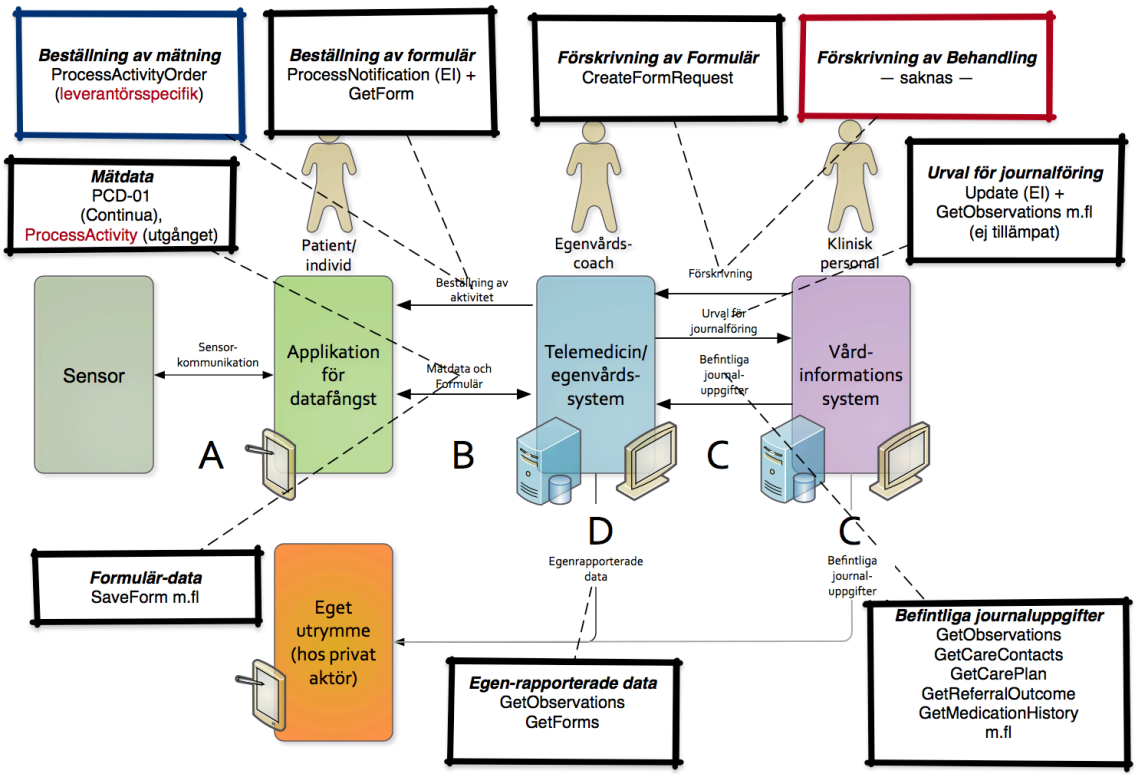
Figur 6 Medicintekniska kodsystem versus kliniska kodsystem

6.5 Befintlig nationella tjänstekontrakt

Det finns en rad nationella specifikationer i Ineras tjänstedomänsportfölj för informationsutbyte (tjänstekontrakt) som ger stöd för referensarkitekturens informationsgränssnitt. Samtliga är baserade på SOAP-standarden för meddelande-paketering. Meddelandeinnehåll är baserat på HL7 Green CDA, Socialstyrelsens NI eller i ett fall IHE.

Två av användningsfallen saknar stöd och tillämpning i den nationella tjänstekontraktsportföljen: Förskrivning och Förskrivning av aktivitet. En extern part (leverantör) har tagit initiativ till öppna tjänstekontrakt för Förskrivning av aktivitet. De ingår inte i Ineras nationella utbud.

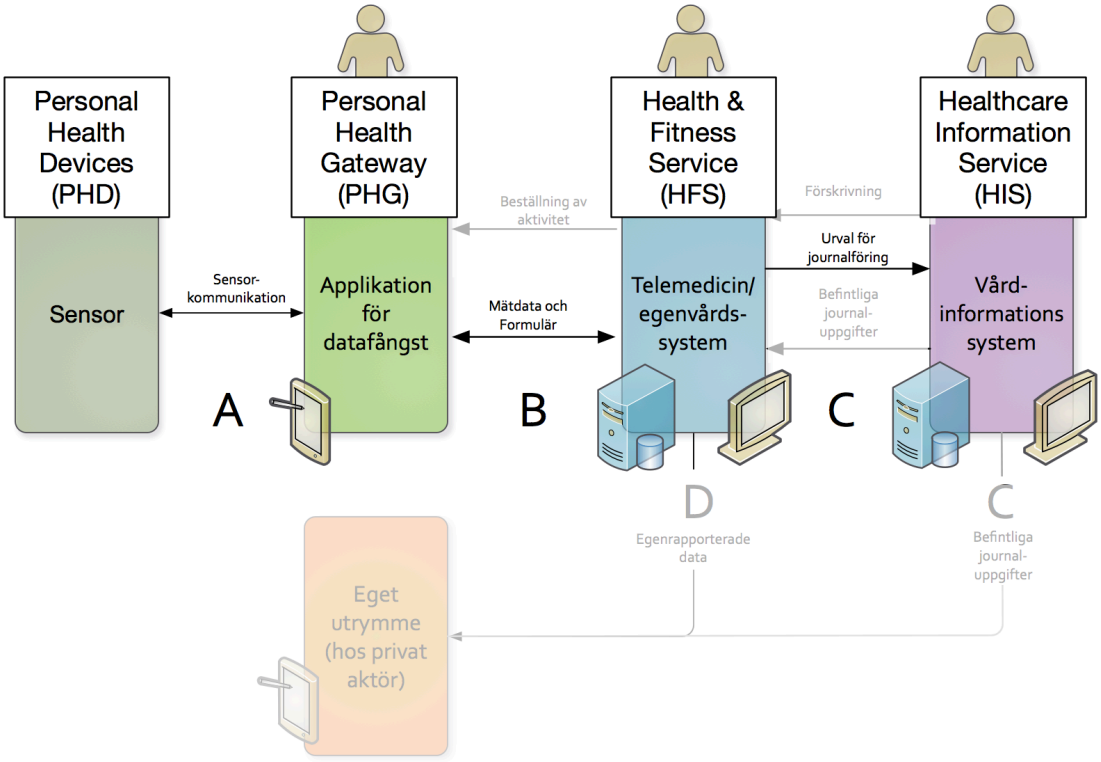
Figuren nedan relaterar referensarkitekturen till nationella tjänstekontrakt.



Figur 7 Användningsfall och informationsutbyten - Nationella tjänstekontrakt (RIVTA SOAP, IHE SOAP)

6.6 Continua design guidelines

Byggblocken och deras informationsutbyten är – liksom den nordiska referensarkitekturen [NordiskRA] - baserade på Continua design guidelines referensarkitektur för ”Personal connected health” [Continua]. Figuren nedan visar hur den svenska referensarkitekturen relaterar till Continua design guidelines referensarkitektur. Användningsfall i nedtonad text saknar stöd i Continua Design Guidelines 2017.



Figur 8 Byggblock och informationsutbyten i den svenska referensarkitekturen med motsvarighet i Continua Design Guidlines 2017

Den svenska referensarkitekturen kommer även fortsättningsvis att behöva vara en utökning av Personal connected health alliance [Continua] arbete. Dels behöver den kunna uttrycka krav och regler som ännu inte nått internationell profilering och dels behöver den användas för att förankra behov av att vidareutveckla Continua Deisgn Guidelines.

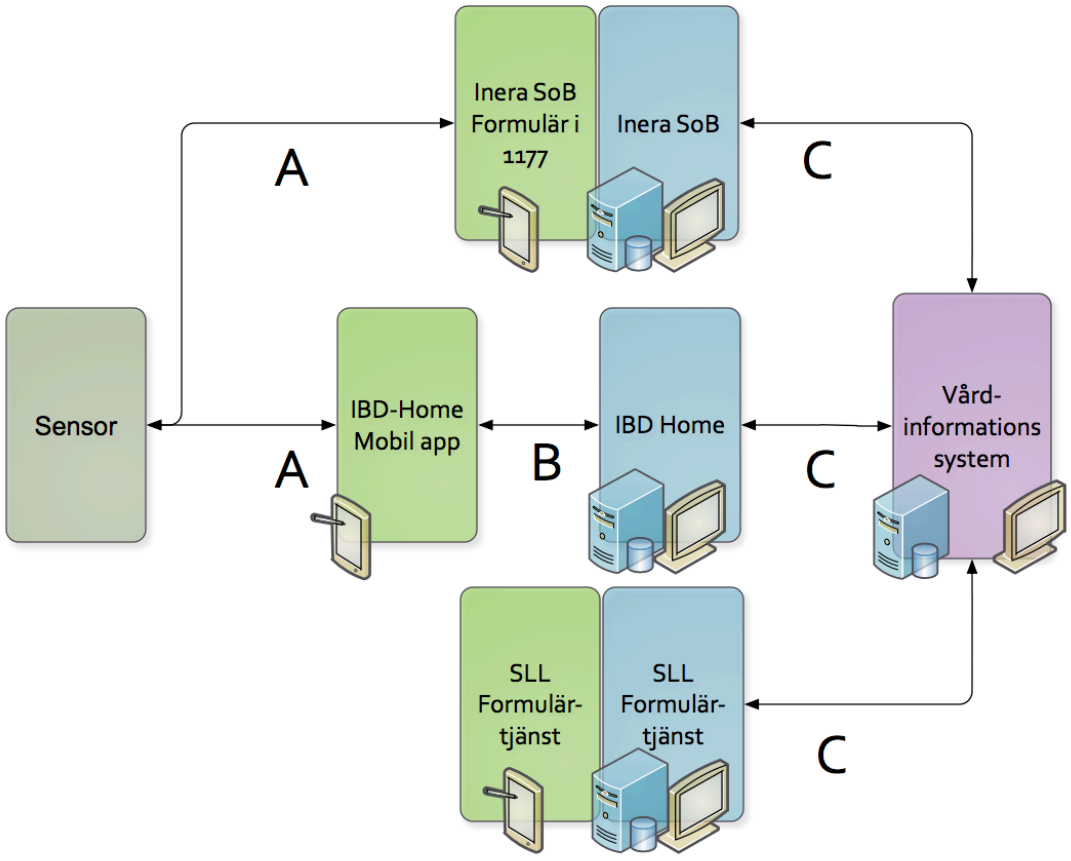
Personal connected health alliance (PCHA) blir därmed – i sin roll som förvaltare av Continua guidelines [Continua] – en strategisk medlemsorganisation för Sveriges kommuner och landsting. SKL behöver aktivt driva frågor mot PCHA när prioriterade användningsfall saknas eller saknar FHIR-stöd. Likaså om det finns hinder för att tillämpa en guideline i den svenska arkitekturen.

6.7 Konsolidering

Referensarkitekturen ger stöd för en gradvis (förutspådd) konsolidering av dagens diagnos-bundna egenvårdslösningar till mer generella egenvårdsplattformar. De tekniska grundstrukturer som tillämpas behöver vara gemensamma med andra tillämpningsområden, såsom första linjens vård, digitala vårdmöten (video, formulär, chat) och kliniskt beslutsstöd (gemensam beslutsstödskomponent).

En sådan utveckling kommer att behöva pågå under lång tid och i takt med att användningen av digitala egenvårdstjänster ökar.

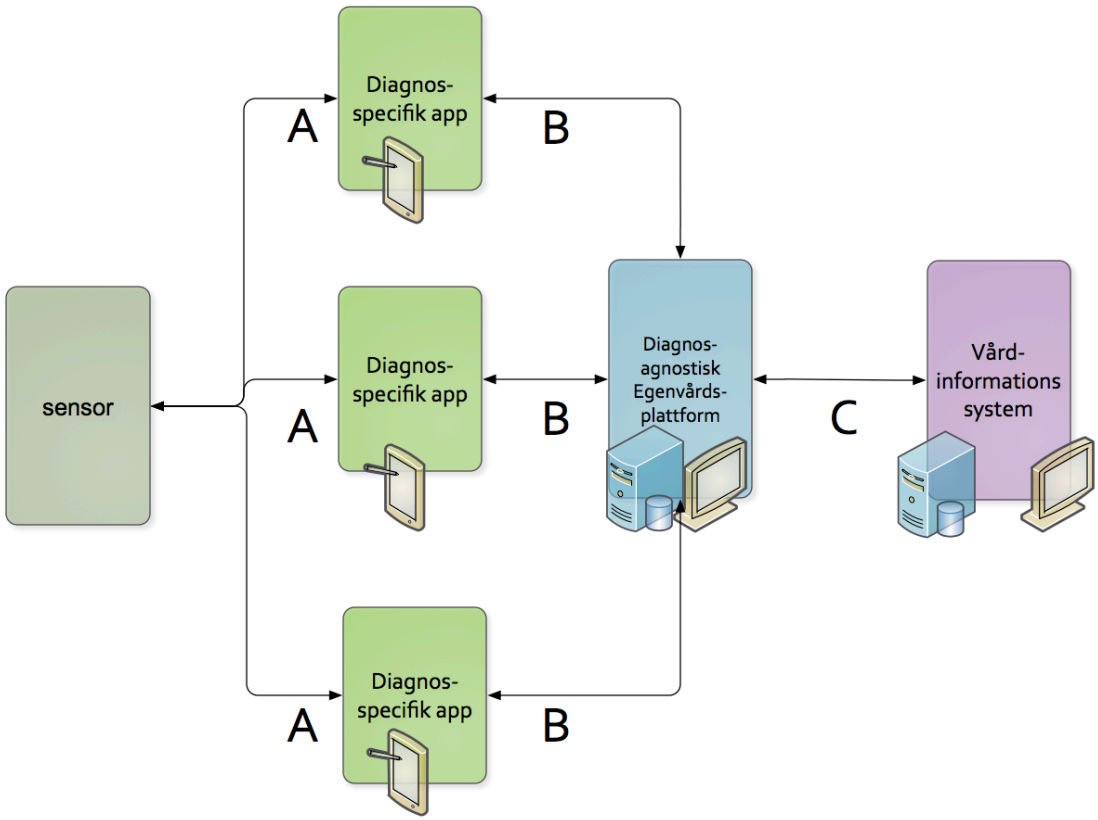
Figuren nedan illustrerar översiktligt några av de telemedicin/egenvårdssystem som skulle kunna vara i användning inom ett landsting. I takt med att floran av telemedicin/egenvårdssystem som används inom huvudman ökar, kan behovet av konsolidering bli allt mer påträngande.



Figur 9 Nuläge - diagnos- eller funktionsspecifika telemedicin/egenvårdsystem

En långsiktig och bred tillämpning av digitala tjänster inom telemedicin/egenvård förutsätter att mängden system kan minskas. Det innebär troligen en strävan mot mer generella telemedicin/egenvårdsystem än de – ofta diagnosspecifika – som används idag. Genom att följa referensarkitekturen vid upphandlingar och integrationer, skapas utrymme för en framtida konsolidering mer minimala dominoeffekter på de integrationer som skapats kring varje specifikt telemedicin/egenvårdssystem.

Figuren nedan visar schematiskt resultatet av konsolidering. Ansatsen bygger på att vårdinformationssystemet inte påverkas av konsolideringen, som därmed kan pågå under lång tid.



Figur 10 - Målbild - funktions- och diagnosgemensamt system för telemedicin/egenvård

6.8 Specifika krav

6.8.1 IT4 – Lös koppling

1. Landsting, regioners och kommuners gemensamt utpekade organ tillhandahåller gemensamma specifikationer (profiler) för informationsutbyten i enlighet med referensarkitekturen
2. De gemensamma specifikationerna baseras på internationell standardisering och profilering inom området. Tillämpade standarder och profileringsarbeten ska ha internationellt brett stöd i produkter eller strategier bland marknadens aktörer inom telemedicin.
    a. HL7 FHIR är tillsvidare föredragen standard för interoperabilitetsprofiler inom områdena B, C och D
    b. PHCA [Continua] är tills vidare vald som primär profileringsorganisationen för samtliga områden. För område B, C D gäller Continua Design Guidelines för de anvädningsfall som har stöd av FHIR-baserade profiler.

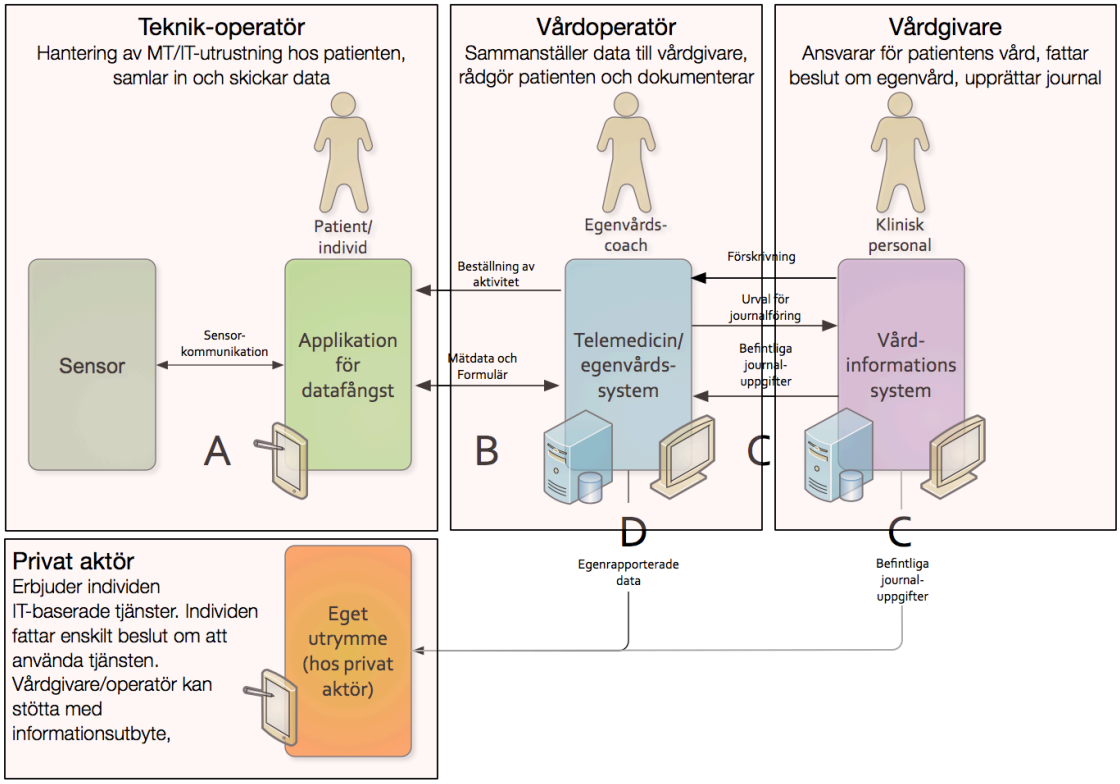
   c. För de användningsfall som saknar stöd i Continua Design Guidelines eller där FHIR-baserade profiler saknas ska landsting, regioners och kommuners gemensamt utpekade organ i första hand verka för att PCHA inför FHIR-baserade profiler för saknade användningsfall, i andra hand utveckla svenska FHIR-profiler (gäller inte område A) och i tredje hand tillämpa befintliga nationella specifikationer för informationsutbyte (SOAP-baserade tjänstekontrakt).

3. Upphandling, utveckling och anpassning av lösningar inom telemedicin som omfattar hela eller delar av arkitekturens byggblock (funktioner och informationsutbyten) bör ställa krav på att lösningar redovisar följsamhet till referensarkitekturen (se exempel i avsnitt
4. Upphandling, utveckling och anpassning av lösningar inom telemedicin som omfattar hela eller delar av arkitekturens byggblock (funktioner och informationsutbyten) ska ställa krav på certifiering (i förekommande fall) och interoperabilitet i enlighet med de profiler och rutiner som gemensamt utpekade organ tillhandahåller.
5. Nationellt fastställda kliniska kodsystem ska användas C-gränssnittet. Nationellt fastställda medicintekniska kodsystem ska användas i B- och D-gränssnitten.

7. Organisatorisk vy

Organisatoriskt kan leveransen av ordinerad egenvård vara uppdelad mellan olika aktörer. På en öppen marknad för sådana aktörer kan varje aktör optimera sin leverans genom det mest ändamålsenliga IT-stödet. Referensarkitekturen visar hur negativa sidoeffekter orsakade av brister i informationsflödet mellan aktörernas IT-stöd kan undvikas.

Figuren nedan illustrerar ett exempel på aktörer inom ordinerad egenvård och vilka byggblock i arkitekturen som motsvarar respektive aktörs huvudsakliga IT-stöd. Genom att varje aktörs IT-stöd följer referensarkitekturens principer säkerställs ett sömlöst informationsflöde utan behov av kundanpassade integrationer.



Figur 11 Organisationer och IT-stöd inom ordinerad egenvård

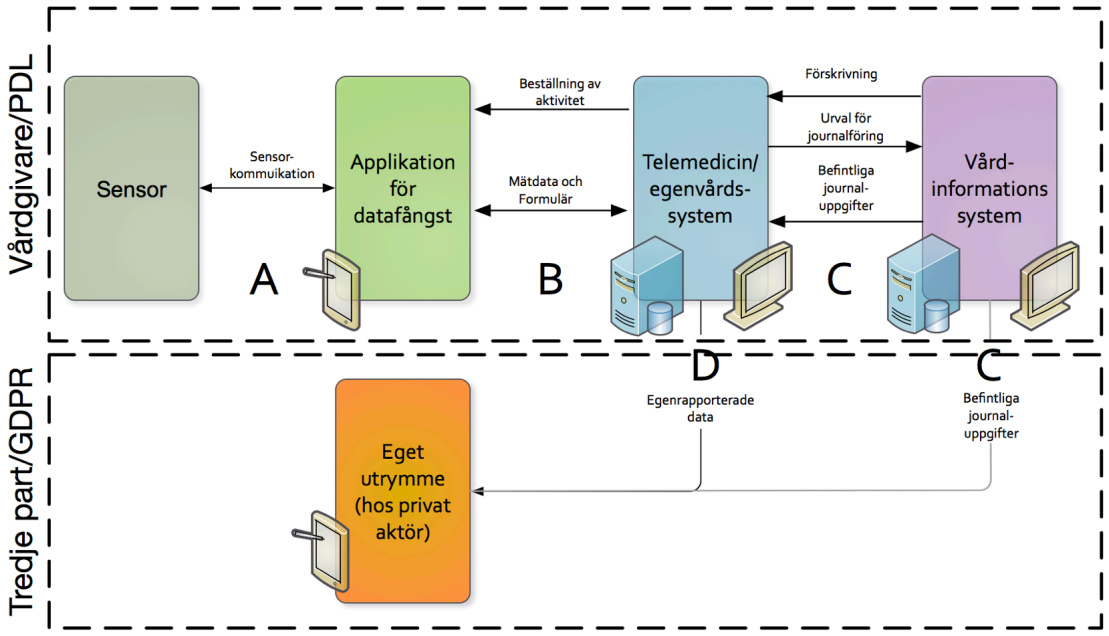
8. Legal vy

8.1 Ansvaret för personuppgiftsbehandlingen

För förskriven egenvård gäller som princip att förskrivande vårdgivare är personuppgiftsansvarig för personuppgiftsbehandlingen i alla funktionella byggblock utom Eget utrymme. Hela informationsflödet regleras av Patientdatalagen. Som konsekvens ska överföring av patientens registrerade information till egenvårdslösningen inte föregås av samtycke.

Det finns exempel på egenvårdslösningar (Eget utrymme) som patienten väljer att använda efter eget beslut, för s.k. individ-beslutad monitorering. Sådana lösningar kan möjliggöra överföring till Telemedicin/egenvårdssystem. Det är ett användningsfall som inte regleras av denna version av referensarkitekturen.

Figuren nedan illustrerar lagrum och personuppgiftsansvarets fördelning utgående från arkitekturens byggblock.



Figur 12 Illustration till legal vy

8.1.1 Kommentar avseende sammanhållen journalföring

Informationsutbytet i gränssnitten A, B, C och D sker inom en vårdgivares personuppgiftsansvar. När det gäller utbyte av *Befintliga journaluppgifter* mellan ett *Vårdinformationssystem* och ett *Telemedicin/egenvårdssystem* kan avgränsning till samma vårdgivare vara kliniskt begränsande. Kanske hade patientens hela (nationella) vårdhistorik varit en värdefull resurs för vårdplanens utförande. Men det legala utrymmet är begränsat till det som erbjuds av PDL inom *Sammanhållen journalföring*: direktåtkomst. Nyttan uppstår först när vårdgivaren med ansvar för telemedicin/egenvårdsystemet har möjlighet att ladda ner och

bearbeta befintliga journaluppgifter under förloppet av den ordinerade egenvården, vilket inte är möjligt inom ramen för sammanhållen journalföring. Därför begränsar referensarkitekturen utbyte av *Befintliga journaluppgifter* mellan ett *Vårdinformationssystem* och ett *Telemedicin/egenvårdssystem* till att ske inom en personuppgiftsansvarig vårdgivare.

8.1.2 Kommentar angående patientens/individens informationsåtkomst

Eftersom *Applikation för datafångst* används inom en vårdrelation (ordinerad) och under en personuppgiftsansvarig vårdgivares ansvar, begränsar lagstiftningen möjligheterna till informationsdelning med patienten till enskilds direktåtkomst. Användningsfallen i B-gränssnittet rör ju främst inrapportering, men ”Beställning av aktivitet” innebär att patienten genom *Applikation för datafångst* får tillgång till information om ordinerade formulär- och mätdataaktiviteter. Den informationsdelningen faller under enskilds direktåtkomst.

Informationsdelning genom överföring till tjänst med *Eget utrymme* innebär däremot med nödvändighet att information lämnas ut till individen själv eller till den tredje part som ansvarar för skyddet av personuppgifter i tredjepartstjänsten. Det finns därför – till skillnad mot enskilds direktåtkomst/PDL - inga legala begränsningar för hur den utlämnande informationen tekniskt får behandlas eller delas vidare till andra personer (ombud) och tjänster, utöver vad som regleras genom Dataskyddsförordningen [GDPR].

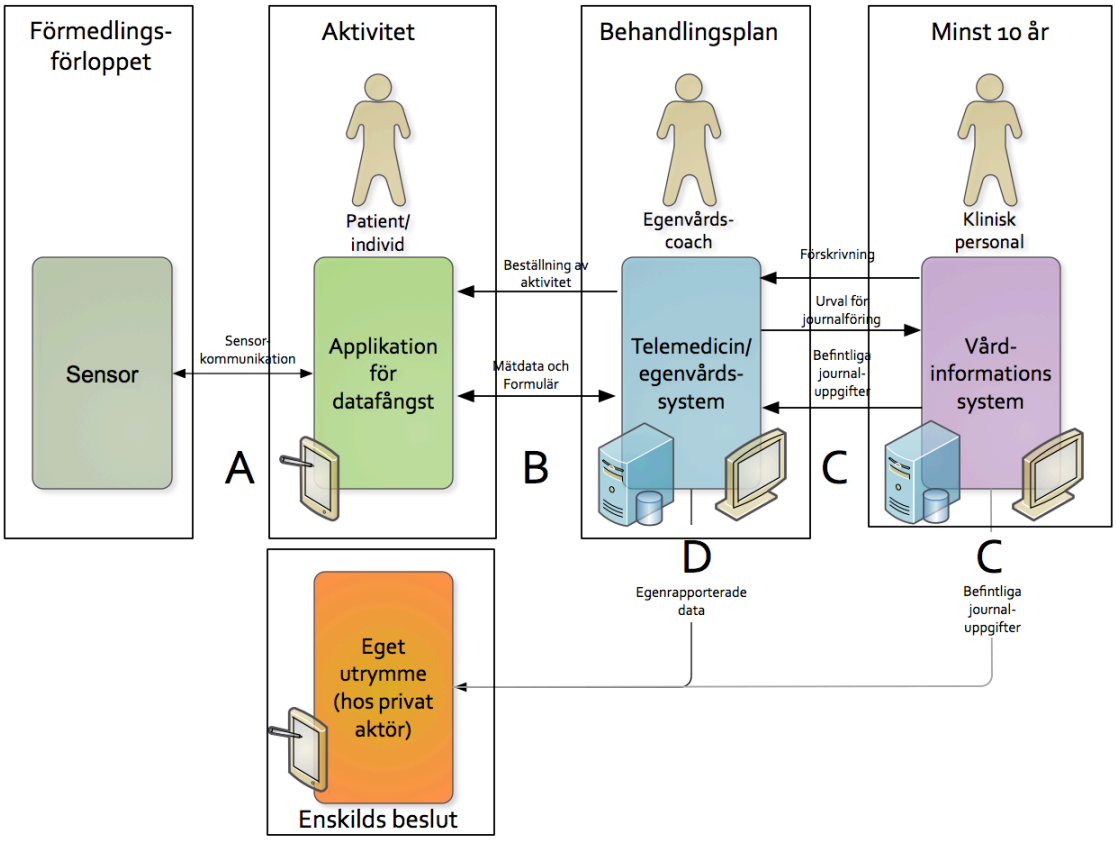
8.1.3 Datalagring och Journalföringsplikt

De mätvärden och formulärdata som vårdgivaren samlar in och lagrar i en egenvårdslösning faller under patientdatalagen, men betraktas inte som journaluppgifter. De ska därför – som huvudprincip - gallras efter att egenvårdsplanen är slutförd.

Endast sådan information som utgör underlag för kliniska beslut behöver journalföras. Det sker genom överföring vis informationsgränssnitt för användningsfall ”Urval för journalföring” (C).

Om patienten erbjuds digitalt utlämnande av egenregistreread information (dataportabilitet) behöver det därför ske innan gallring. Att förvara uppgifterna enbart i syfte att möjliggöra export till enskild, anses inte vara ett legitimt ändamål för personuppgiftsbehandling hos en vårdgivare.

Figuren nedan illustrerar maximal livslängd på personuppgifter för de olika funktionella byggblocken.



Figur 13 Gallrings- och lagringsskyldighet

När utlämnande till eget utrymme är aktuellt, bör överföringen tekniskt arrangeras enligt protokoll som möjliggör för den enskilde att agera under pseudonym i den tjänst/app som erbjuder det egna utrymmet. På så sätt kan – om det ligger i den privata aktörens intresse – den enskilde erbjudas möjlighet att registrera kontot under pseudonym. Informationen som lämnas ut till kontot ska därför inte heller omfatta strukturerade uppgifter som uttryckligen bidrar till att identifiera den enskilde (t.ex. namn, adress, personnummer).

8.1.4 Produktmärkning som medicinteknisk produkt

Produktmärkning som medicinteknisk produkt påför leverantörer av IT-lösningar med motsvarighet i ett eller flera byggblock i arkitekturen ett tillverkaransvar. Det är en grundtrygghet för vårdgivare att använda sig av produkter med produktmärkning som medicinteknisk produkt, under förutsättning att märkningen är standardiserad av EU. Märkningen innebär bland annat att de är testade ur patientsäkerhetssynpunkt för ett visst användningsområde. Leverantören kan inte friskriva sig från ansvar för t.ex. personskada inom produktens användningsområde.

8.2 Specifika krav

8.2.1 TM1 – Uppgiftsminimering

1. Vid överföring till Eget utrymme (utlämnande på medium för ADB) ska Telemedicin/egenvårdssystemet respektive Vårdinformationssystemet undanta strukturerade uppgifter som uttryckligen bidrar till att identifiera den enskilde (t.ex. namn, adress, personnummer).

8.2.2 TM2 – Lagringsminimering

2. Ett Telemedicin/egenvårdssystem ska ha rutiner som säkerställer att patientuppgifter gallras i anslutning till att behandlingsplanen avslutats
3. En Applikation för datafångst ska ha rutiner som säkerställer att personuppgifter gallras så snart en monitorerings/formuläraktivitet är utförd och rapporterad till Telemedicin/egenvårdsystemet.

8.2.3 TM3 – Personuppgiftsansvar

4. Förskrivande vårdgivare är personuppgiftsansvarig för den behandling av personuppgifter som sker i samtliga byggblock, med undantag av Eget utrymme.
5. Förskrivande vårdgivare är personuppgiftsansvarig för samtliga informationsutbyten, inkluderande utlämnande till Eget utrymme
6. Befintliga journaluppgifter kan bara överföras inom en personuppgiftsansvarig vårdgivare i gränssnittet C, avseende utbyte mellan telemedicin/egenvårdsystem och vårdinformationssystem.
7. Samtliga IT-produkter som omfattas av de funktionella byggblocken (6.2) och där märkning som medicinteknisk produkt är tillämpbar ska vara märkta som medicintekniska produkter enligt gällande regelverk inom EU.

8.2.4 TM4 – Dataportabilitet

8. Telemedicin/egenvårdsystem bör stödja D-gränssnittet för ADB-utlämnande till Eget utrymme.

inera

9. Informationssäkerhetsvy

Det finns många typer av säkerhetsrisker som behöver beaktas vid konstruktion av applikationer och informationssystem som hanterar känsliga personuppgifter. Denna referensarkitektur är avgränsad till risker som relaterar till informationsutbyte mellan systemkomponenter som ligger under olika ansvarsgränser. Ansvarsgränser syftar här på olika juridiska personers ansvar för skydd av personuppgifter i samband med informationsutbyte.

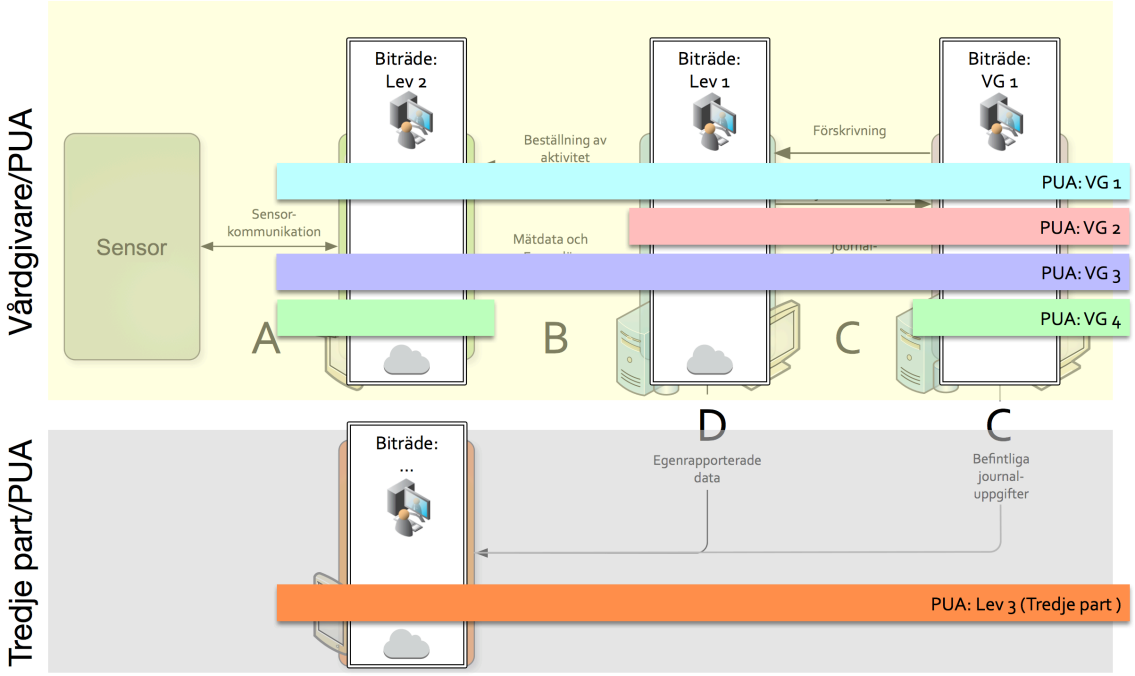
Dessa organisationer kan vara personuppgiftsansvariga eller personuppgiftsbiträden för de IT-komponenter som realiserar arkitekturens byggblock. I och med den nya dataskyddsförordningen [GDPR] minskar skillnader i ekonomiskt risktagande mellan biträden och personuppgiftsansvariga, i förhållande till tidigare lagstiftning (PUL). Därför utgår referensarkitekturen ifrån ett antagande om att organisationer med personuppgiftsansvar och organisationer i biträdesroll har samma intressen i hur risker relaterade till informationsutbyte dem emellan kan minskas.

9.1 Intrångspunkter, risker och åtgärdsbehov

Figuren nedan illustrerar ett exempel på fördelning av roller mellan personuppgiftsansvariga och biträden i förhållande till arkitekturens byggblock. I exemplet är Vårdinformationssystemet installerat inom en huvudmans egen förvaltnings- och it-driftsverksamhet. Huvudmannen är vårdgivare och personuppgiftsansvarig för sin informationshantering i Vårdinformationssystemet, men samtidigt biträde till andra vårdgivare med vårdavtal som journalför i samma systeminstallation.

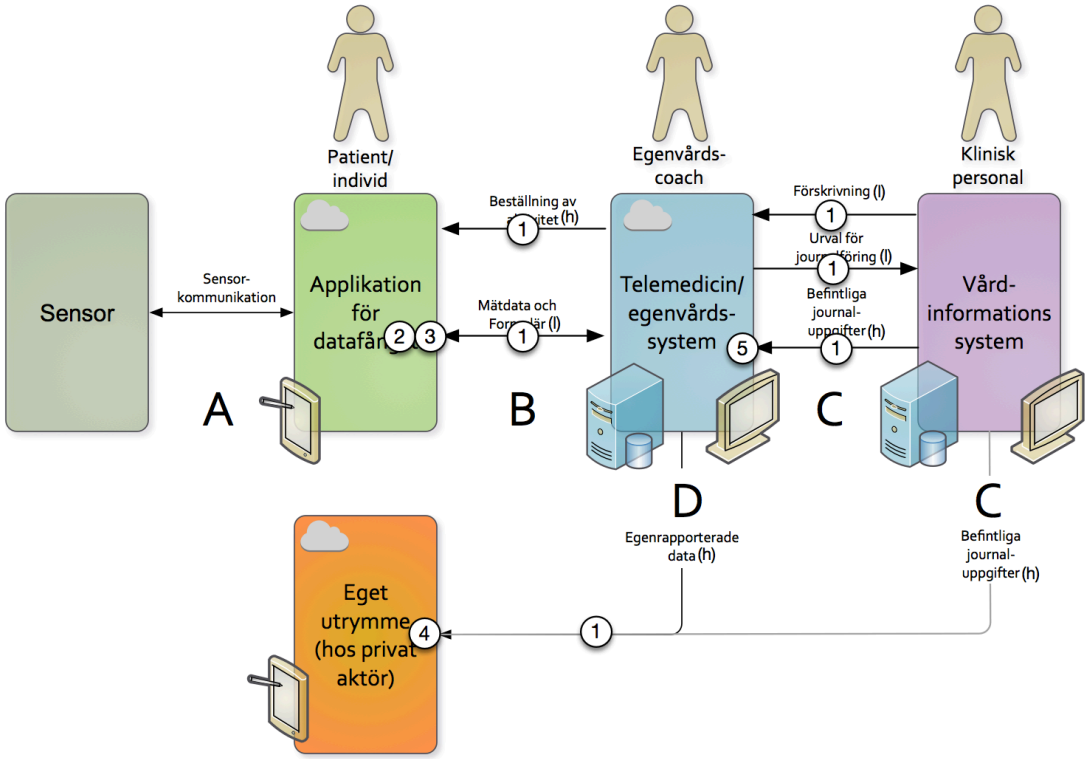
Telemedicin/egenvårdsystemet är en SaaS-tjänst [SaaS] som tillgängliggörs av en leverantör (Lev 1). Systemet används av tre av de fyra vårdgivare (VG1, VG2 och VG3) som arbetar på uppdrag av huvudmannen (VG 1).

Telemedicin/egenvårdsystemet har flera anslutna Applikationer för datafångst. En av dem visas i figuren och även den tillhandahålls som SaaS-tjänst [SaaS] av ytterligare en leverantör (Lev 2).



Figur 14 Exempel på fördelning av personuppgifts- respektive biträdesansvar

Risker uppstår när systemen öppnas upp för informationsutbyte med andra system. Tabell 5 sammanfattar sådana risker och olika åtgärdsmöjligheter. Riskerna i tabellen är numrerade enligt figuren nedan. Analysen bygger på att en tjänst hämtar information från källan, det vill säga att källan är tjänsteproducent [T-boken]. Det är rådande praxis så väl nationellt [T-boken] och internationellt [Continua]. Undantaget är användningsfallet ”förskrivning”. Detta markeras i Figur 15 för respektive informationsutbyte med symbolerna ”(l)” för lämna och ”(h)” för hämta.



Figur 15 Intrångspunkter i riskanalysen

Analysen klassificerar åtgärdsbehovet som Lågt, Högt eller Kritiskt. Ju större del av populationen som är i riskzonen för ett integritetsbrott, desto högre klassning. Klassningen väger även in patientsäkerhetsrisker.

Tabell 5 Analys av risker och åtgärdsbehov

	Risk	Exempel	Åtgärdsbehov	Åtgärdsmöjligheter
1	Läckage genom avlyssning av överförings-kanal (B, C, D)	Överförings-kanalen (B) mellan Lev 2 och Lev 1 avlyssnas på internet.	***Kritiskt***, särskilt då utbytet sker över öppet nät	Kryptering av överföringskanalen genom SSL/TLS, via nycklar från godkända utfärdare [IAM-RA]
2	Intrång i Applikation för datafångst som ger möjlighet att sända falska	Lev 2 är ”hackad”. Falska formulär-svar når tjänst hos Lev 1 och ev.	***Lågt***, eftersom förväntad patientsäkerhets- eller integritetsskada är låg. Falska värden upptäcks tidigt, t.ex.	Tjänsteproducent för Telemedicin/egenvårdssystemet ska säkerställa att informationsöverföring begränsas till vårdgivare med adekvat biträdesrelation till

	data till anslutet telemedicin/ egenvårds-system genom att missbruka överföringska nal B	VG1 (biträde) (B, C).	genom att de är orimliga, har fel frekvens, eller är kopplade till en patient som saknar aktiv vårdplan.	leverantören av Applikation för datafångst samt till patienter med en aktiv aktivitetsbeställning. När patienten/individen är användaren av tjänsten kan mottagande tjänsts mottagningspunkt skyddas genom OAUTH [IAM-RA]. Då begränsas möjligheten att generera falska data till de patienter som är aktiva, samt att data endast når fram om ”hackaren” tillskansar sig aktuella OAUTH-nycklar.
3	Intrång i Applikation för datafångst som ger möjlighet att läsa patientdata från anslutet telemedicin/ egenvårds-system genom att missbruka överföringska nal B. Dörren står då vidöppen för alla patientuppgift er för samtliga patienters formulär vars vårdgivare använder	Lev 2 är ”hackad”. Obehörig får tillgång till patientdata lagrade i telemedicin/ egenvårds-systemet hos Lev 1 från VG 1 och 3.	***Högt***. Gränssnitt B möjliggör läsning av obesvarade (väntande) formulär och även ifyllda, men ännu ej rensade formulär. Det ger inte möjlighet till systematisk hämning av data eftersom det bara lagras data för patienter med en vårdplan. B-gränssnittet stödjer inte läsning av inrapporterad mätdata.	Tjänsteproducent för Telemedicin/egenvårdssy stemet ska säkerställa att informationsåtkomst begränsas till information från vårdgivare med adekvat biträdesrelation till leverantören av Applikation för datafångst. Eftersom patienten/individen är användaren av Applikation för datafångst Telemedicin/ egenvårdsystemet begränsa åtkomsten till data som rör patienter som för tillfället är aktiva användare av den aktuella Applikationen för datafångst. Det kan ske med hjälp av OAUTH [IAM-RA]. Åtkomst förutsätter dessutom att ”hackaren” tillskansar sig

	den aktuella telemedicin/ egenvårds-tjänsten. Tjänsten håller dock bara patient-data för patienter med aktiva formulär.			aktuella OAUTH-nycklar. Skadan av eventuella uthämtade personuppgifter kan ytterligare begränsas genom att Telemedicin/ egenvårdsystemet inte röjer patientens identitet för Applikationen för datafångst. Det är också en åtgärd som kan realiseras med hjälp av OAUTH [IAM_RA].
4	Intrång i tjänst för Eget utrymme som ger möjlighet att läsa patientdata från anslutet Vårdinformati ons-system genom att missbruka överföringska nal C och D. Dörren står då vidöppen för alla patientuppgift er för samtliga patienter vars vårdgivare stödjer överföring till den aktuella tjänsten med Eget utrymme från sitt journal-system.	Lev 3 är ”hackad”. Obehörig får tillgång till patientdata lagrade i Vård-informations-systemet hos VG 1 (C) och telemedicinsyst emet (D)	***Kritiskt***. Vårdinformations-systemet kan täcka en stor regions samtliga patienter och en andel utomlänspatienters journaluppgifter sedan många år tillbaka. Tjänsten för Eget utrymme [SaaS] kan dessutom vara anslutet till många huvudmäns och upphandlade privata vårdgivares Vårdinformations-system. Patienter som är användare av en tjänst för Eget utrymme kan vara i van-maktssituation och därigenom ha aktiverat utlämnande av journaluppgifter på ofrivillig basis.	Tjänsteproducent för Vårdinformations-systemet ska säkerställa att informationsåtkomst begränsas till information från vårdgivare med adekvat biträdesrelation till leverantören av Telemedicin/egenvårdslö sningen. Åtkomstskydd genom OAUTH [IAM-RA] på kanal B och C vid ADB-utlämnande till enskild ger följande riskhantering: a: Information som läcker ut kan inte enkelt knytas till en fysisk person, förutsatt att individen har möjlighet till konto under pseudonym i aktuell tjänst för Eget utrymme b: Information kan endast läcka ut för individer som har ett aktivt konto i den aktuella tjänsten med Eget utrymme (typiskt en

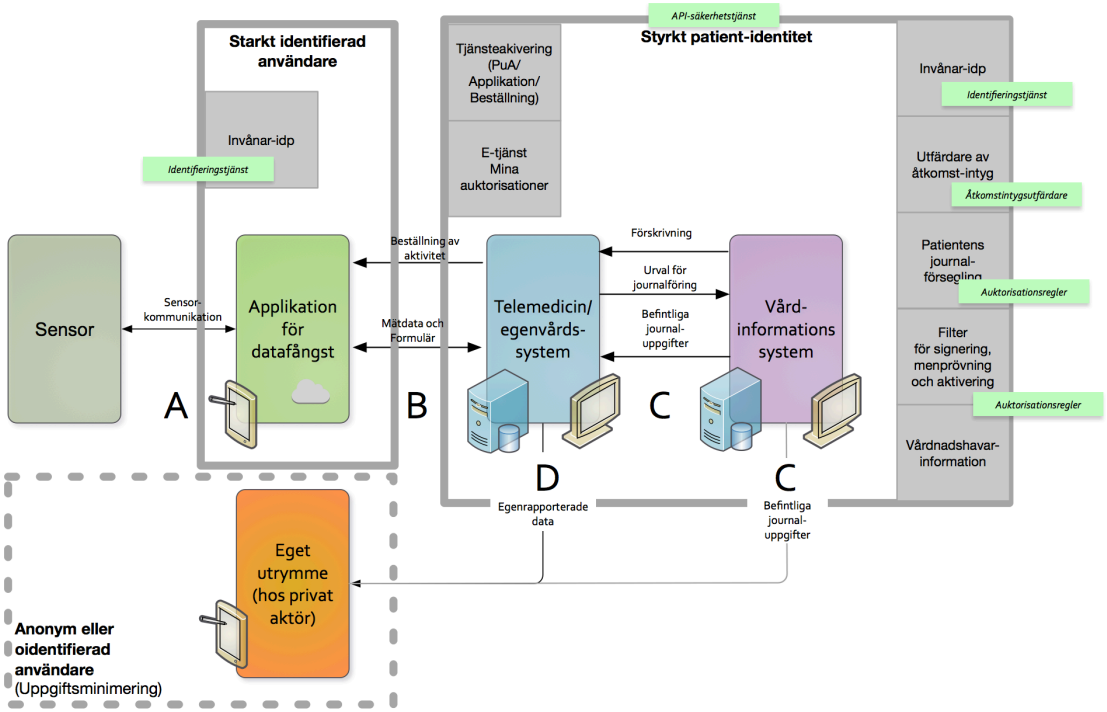
			Information som inte är menprövad kan komma till patientens eller anhörigs kännedom.	starkt begränsad del av populationen) och där individen dessutom aktiverat möjlighet att ta emot ADB-utlämnade journal-uppgifter för specifika vårdgivare För att hindra oönskad informationsåtkomst i vanmaktssituation ska vårdinformations-systemet filtrera information för utlämnande baserat på ett nationellt förseglingsregister. För att undvika läckage av icke menprövad information ska mekanism säkerställa att information som inte menprövats filtreras bort av den OAUTH-skyddade resursen.
5	Intrång i Telemedicin/ egenvårds-system som ger möjlighet att läsa patientdata från anslutet Vårdinformati ons-system genom att missbruka överförings-kanal C (Befintliga journaluppgift er).	Lev 1 är ”hackad”. Obehörig får tillgång till patientdata lagrade i Vård-informations-systemet hos VG 1 (C) för VG1, 2 och 3.	Kritiskt. Vårdinformationssy stemet kan täcka en stor regions samtliga patienter och en andel utomlänspatienters journaluppgifter sedan många år tillbaka. Telemedicin/ Egenvårdssystemet [SaaS] kan dessutom vara anslutet till många huvudmäns och upphandlade	Tjänsteproducent för Vårdinformations-systemet ska säkerställa att informationsåtkomst begränsas till information från vårdgivare med adekvat biträdesrelation till leverantören av Telemedicin/egenvårdslö sningen. Ytterligare åtkomstskydd genom att Vård-informations-systemet begränsar Telemedicin/ egenvård-systemets åtkomst till information som rör patienter med en

	Dörren står då vidöppen för alla patientuppgifter för samtliga patienter vars vårdgivare stödjer överföring till det aktuella systemet för Telemedicin/ Egenvård.		privata vårdgivares vårdinformations-system.	aktiv förskrivning i det aktuella Telemedicin/ egenvård-systemet. Det leder till en kraftig reducering av antalet patienter som riskerar integritetsskada vid intrång i ett Telemedicin/egenvårdssystem.

Åtgärdsmöjligheterna sammanfattas i avsnitt 9.3.

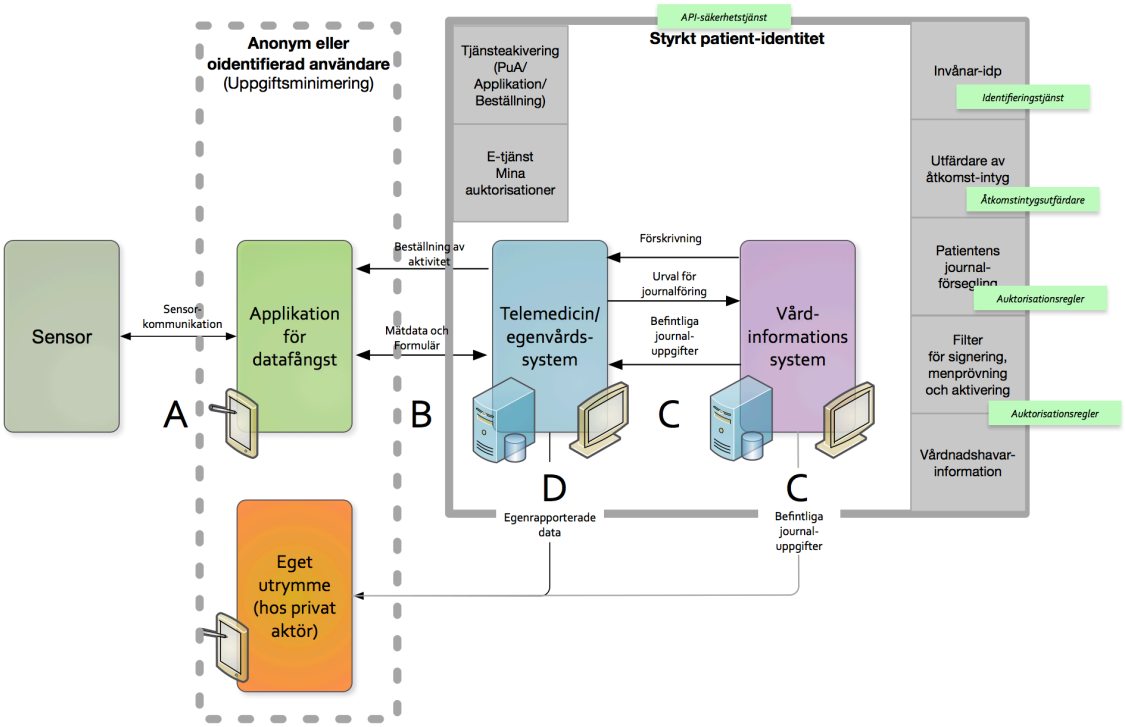
9.2 Identifiering av användaren

Om patient/individ-tjänsten är en Applikation för datafångst med lagring av personuppgifter i en server-miljö utanför den enskildes enhet, ska applikationen ha stöd för att starkt identifiera sina användare. En tjänst med datalagring som ligger under vårdgivarens personuppgiftsansvar kan inte erbjuda konton under pseudonym eftersom lagring endast är legalt möjlig om den enskildes folbokföringslandsting kan agera personuppgiftsansvarig. Den enskildes identitet (personidentitet) är en förutsättning för att folkbokföringslandsting ska kunna fastställas. Figur 16 illustrerar detta förhållande. Gröna etiketter refererar begrepp ur [IAM-RA]. Grå rektanglar symboliserar tekniska komponenter som beskrivs i avsnitt 10.1.



Figur 16 Identifieringsbehov vid lagring i personlig enhet eller SaaS-tjänst utan lagring

Om Applikation för datafångst enbart lagrar personuppgifter i den enskildes enhet – kan applikationen samla in och lokalt lagra uppgifterna (formulär, mätvärden) utan att individen behöver autentiseras. När de lokalt lagrade uppgifter ska föras över från enheten via B-gränssnittet, kommer API-säkerhetstjänsten (via sin Åtkomstintygsutfärdare [IAM-RA]) att avkräva en stark autentisering. Tjänsten Åtkomstintygsutfärdare kommer då att tillhandahålla ett användargränssnitt där patienten får godkänna att aktuell Applikation för datafångst för över lokalt lagrad information till aktuell vårdgivare. Ett sådant godkännande förutsätter att patienten autentiseras starkt. Åtkomstintygsutfärdaren agerar därför i rollen Service provider [IAM-RA] i förhållande till en Identifieringstjänst [IAM-RA] – det vill säga sin Invånar-IDP – och kan på så sätt säkerställa för vem åtkomstintyget utfärdas. Åtkomstintyget – men inte patientens identitet – blir sedan tillgängligt för Applikation för datafångst, som därigenom kan genomföra ett API-anrop (gränssnitt B) som skickar mätvärden eller formulär till Telemedicin/egenvårdssystemet via API-Säkerhetstjänsten. Detta gäller även Applikation för datafångst med server-komponent – t.ex. en SaaS-tjänst – om personuppgifter enbart hanteras inom en session. Åtkomstintyget lagras då i sessionen och kan sägas utgöra en pseudonymiserad stark identitet. Figur 17 illustrerar detta förhållande. Gröna etiketter refererar begrepp ur [IAM-RA]. Grå rektanglar symboliserar tekniska komponenter som beskrivs i avsnitt 10.1.



Figur 17 Identifieringsbehov vid lagring i server – exempelvis SaaS-tjänst

Om patient/individ-tjänsten är en tjänst med Eget utrymme finns inga säkerhetsmässiga krav på att den enskilde ska vara starkt identifierad – eller alls identifierad. Den enskildes utlämnade personuppgifter kan lagras i den enskildes mobila enhet, i en servermiljö under konto med pseudonym (användarnamn/lösenord) eller under den enskildes styrkta personidentitet. Det är först när en tjänst eller lokalt installerad app för Eget utrymme ska efterfråga utlämningsbara journal/personuppgifter via API gränssnitt C eller D (befintliga journaluppgifter/egenrapporterad data) som patientens identitet behöver styrkas. Det sker enligt samma flöde som när en Applikation för datafångst ska överföra insamlade formulärdata/mätvärden (se föregående stycke).

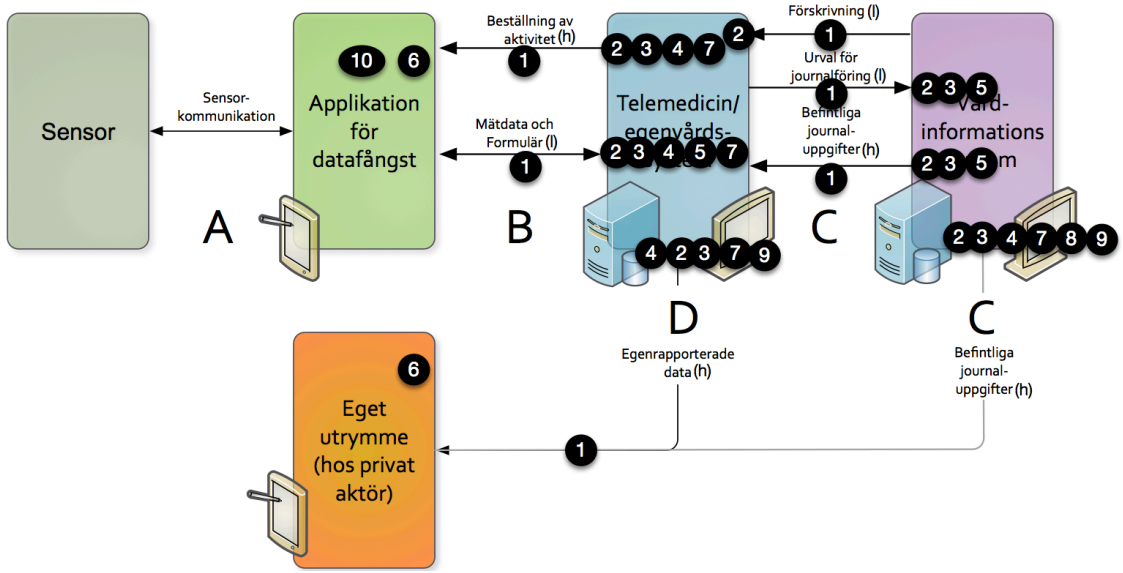
9.3 Specifika krav

Följande specifika krav rör information som utbyts inom vårdgivares personuppgiftsansvar inom ramen för PDL, inklusive ADB-utlämnande från vårdgivare till tjänst för Eget utrymme. Genom att följa kraven har man vidtagit de åtgärder som föreslås i tabellen i avsnitt 9.1.

Varje krav behöver realiseras i ett eller flera av arkitekturens byggblock (se 6.1). Detta illustreras av Figur 18. Beskrivningarna av specifika krav hänvisar till begreppet tjänsteproducent [T-boken]. Vilket byggblock som är tjänsteproducent respektive tjänstekonsument i ett informationsutbyte påverkas av valet av interaktionstyp – ”push”

respektive ”pull”, eller ”lämna” respektive ”hämta”. Valet av interaktionstyp är markerat i Figur 18 efter namnet på respektive användningsfall: ”(l)” betyder lämna och ”(h)” betyder hämta.

Exempelvis är användningsfallet ”Beställning av aktivitet” hanterat som ”hämta” – dvs att Applikation för datafångst efterfrågar beställningar från Telemedicin/egenvådssystemet. Telemedicin/egenvådssystemet (källa) är tjänsteproducent och Applikation för datafångst (mottagare) är tjänstekonsument. För användningsfallet Förskrivning lämnar istället Vårdinformationssystemet förskrivningen till Telemedicin/egenvådssystemet. Telemedicin/egenvådssystemet (mottagare) är tjänsteproducent och Vårdinformationssystemet (källa) är tjänstekonsument.



Figur 18 Informationssäkerhetskrav och byggblock

9.3.1 IT2 – Informationssäkerhet

1. Informationsutbyte sker över ömsesidigt autentiserade krypterade kanaler
2. Tjänsteproducenten ska tekniskt avgränsa informationsutbytet till att gälla ursprungliga tjänstekonsumenter med biträdesavtal som täcker ändamålet för informationsutbytet för minst en av de personuppgiftsansvariga fysiska personer vars information tjänsteproducenten hanterar via aktuellt informationsutbyte[4]. Kravet gäller samtliga tjänsteproducenter.

[4] Detta är ett krav sedan 2013 på tjänsteproducenter för de s.k. journal- och läkemedelstjänstekontrakten

3. Tjänsteproducenten ska logiskt begränsa informationsutbytet till de personuppgiftsansvariga fysiska personer som omfattas av biträdesavtal enligt särskilt krav 2[5]. Kravet gäller samtliga tjänsteproducenter.
4. När informationsutbytet syftar till att samla in eller dela information med enskild och ursprunglig tjänstekonsument är en SaaS-tjänst ska informationsutbytet skyddas med OAUTH [IAM-RA]. Kravet gäller följande flöden: Befintliga journaluppgifter (C) till tjänst för Eget utrymme, Egenrapporterade data (D) till tjänst för Eget utrymme och samtliga B-flöden.
5. Tjänsteproducenter ska avgränsa informationsutbyte till patientuppgifter som har en aktiv aktivitet eller vårdplan i tjänsten som utgör ursprunglig tjänsteproducent. Det vill säga en tjänsteproducent ska inte förmedla uppgifter den fått från en annan tjänsteproducent. Kravet gäller följande flöden: Mätdata och formulär (B), Urval för journalföring (C) och Befintliga journaluppgifter (C).
6. Det ska i alla lägen vara uppenbart för patienten/den enskilde var (på vilken websida) patienten kan återkalla utfärdade OAUTH-tokens (relaterar till 4 och 7). Det ska lösas på ett sätt som inte förutsätter att den enskilde minns för vilka tjänster hen har avgivit åtkomst-medgivanden (OAUTH-tokens).

9.3.2 TM1 – Uppgiftsminimering

7. När informationsutbytet syftar till att samla in eller dela information med enskild och ursprunglig tjänstekonsument är en SaaS-tjänst ska resurs-servern [IAM-RA] varken samla in eller delge strukturerade masterdata-uppgifter som uttryckligen identifierar den enskilde (personidentitet, namn, adress) eller närstående. Tjänstekonsumenter som kräver en starkt autentiserad användare ska istället få dessa uppgifter genom autentisering och slagning mot personuppgiftstjänst. Kravet gäller samma flöden som krav 4.
8. Inför överföring till tjänst för Eget konto ska vårdinformationssystemet genom flöde Befintliga journaluppgifter (C) filtrera baserat på *ett nationellt förseglingsregister* (vanmaktssituation)
9. Vid ADB-utlämnande till tjänst för Eget utrymme (C) ska endast menprövad information lämnas ut. Menprövningen kan vara automatiserad baserat på regler som ansvarig vårdgivaren beslutar över.

9.3.3 IT6 - Samverkan i federation

10. Applikationer för datafångst ska ha stöd för stark identifiering av patienten om applikationen lagrar personuppgifter i server-miljö (ex. SaaS). Identifieringen bör ske

[5] Detta är ett krav sedan 2013 på tjänsteproducenter för de s.k. journal- och läkemedelstjänstekontrakten

via identifieringstjänst [IAM-RA] som är i SSO-federation med den identifieringstjänst som används av API-Säkerhetstjänstens Åtkomstintygsutfärdare [IAM-RA].

11. *Applikationer för datafångst* och tjänst med *Eget utrymme* ska uppfylla kraven i EUs regelverk ”Code of conduct for health apps” [EUCODE]

10. Teknisk vy

Den tekniska vyn beskriver teknisk arkitektur för de krav inom informationssäkerhet och informationsutbyte som behöver vara tillgodosedda för ett säkert och skalbart införande av digitala tjänster inom telemedicin/egenvård. Kraven är motiverade och beskrivna i övriga vyer och sammanfattas i respektive vys avsnitt om ”Specifika krav”.

Den tekniska vyn beskriver också arkitektur för att tillgodose konceptet ”Nationella virtuella tjänster” [T-boken]. Konceptet innebär att aktörer ges tillgång till information på ett sätt som förespeglar förekomsten av en nationell källa (”ett nationellt journalsystem”), trots att källorna i praktiken ska kunna vara specifika per vård- och omsorgshuvudman, per vårdkoncern (ex. nätdoktor) eller per systemleverantör. T-boken beskriver den grundläggande tekniska arkitekturen för konceptet, men ger inte tillräcklig vägledning för specifika användningsfall inom telemedicin. Det gäller exempelvis användning av engagemangsindex i samband med mätdatainsamling.

Under arbetet med referensarkitekturen har olika frågeställningar kommit upp som också speglar behov av förtydliganden i vissa särfrågeställningar relaterade till telemedicin. Några av dem redovisas nedan i syfte att ge exempel på frågeställningar som besvaras i detta avsnitt:

- Kan en enhetsbunden Applikation för datafångst (”native-app”) ansluta direkt till befintliga Telemedicin/egenvårdssystem eller måste en Applikation för datafångst ha en server-komponent för att kunna ansluta? Ett exempel kan vara att skapa anpassad (skräddarsydd) ifyllnad av MQ5D-formulär.
- Var bestäms vilken Applikation för datafångst en patient ska använda? Kan det finnas flera alternativ där patienten själv väljer utifrån egna preferenser – t.ex. välja mellan en regional och en nationellt Applikation för datafångst via formulär?
- Vilka krav ska jag ställa på säker autentisering m.m. för att en tredjeparts patient- eller vårdgivartjänst i molnet ska få ansluta till vårdinformationssystemet eller Telemedicn/egenvårdsysystemet?
- Ska vi hantera anslutning lokalt/regionalt? Det är komplext för oss att etablera infrastruktur och anslutningsrutiner. Kan det nationella hantera det åt oss? Vi vill ju ändå att allt ska hänga ihop i 1177.
- Hur kan jag vara säker på att patienten kan se all information i Journalen trots att egenvård bedrivs i olika Telemedicin/egenvårdsystem hos olika vårdgivare och även kan vara olika mellan diagnosgrupper inom en vårdhuvudman?
- Ska Telemedicin/egenvårdssystemen uppdatera engagemangsindex för varje nytt mätvärde? Om inte – hur kan patienttjänster annars redovisa mätningar eller formulär från patientens alla pågående behandlingar i olika Telemedicin/egenvårdssystem?

10.1 Realisering av skyddsmekanismer

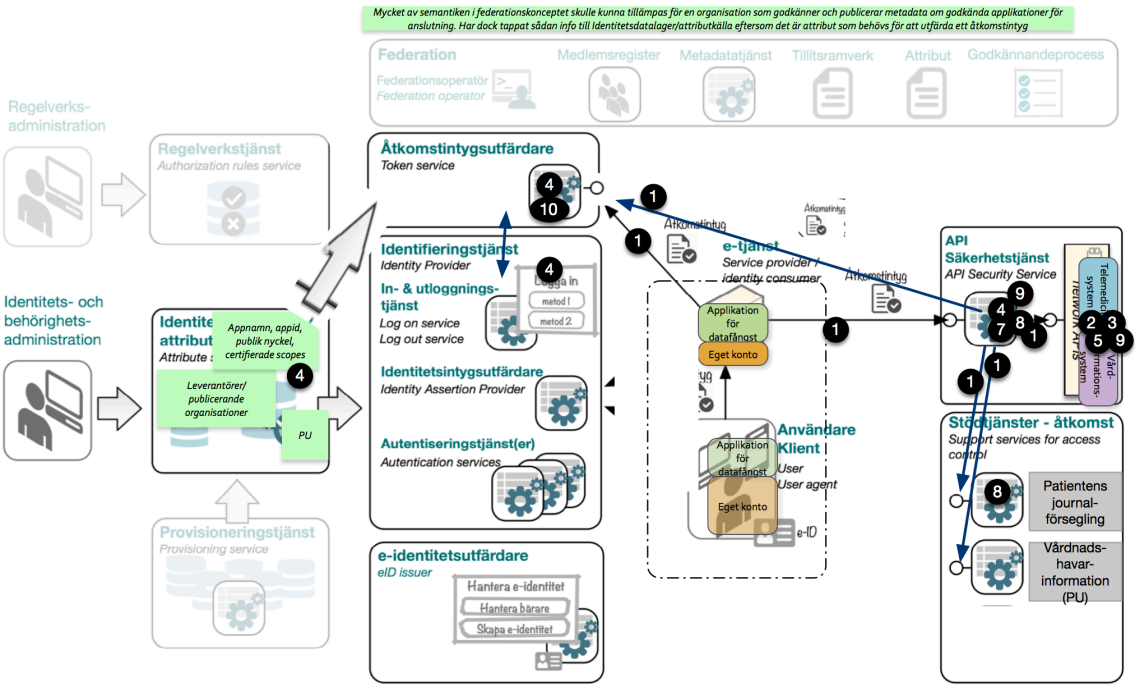
Detta avsnitt beskriver hur ansvaret för de skyddskrav som beskrivs i avsnitt 9.3 fördelas över komponenter i IAM-referensarkitekturen [IAM-RA], vilka infrastrukturella stödtjänster som behövs och hur de funktionella byggblocken påverkas. Figur 19 illustrerar relationen mellan skyddskraven, byggblocken i referensarkitektur för telemedicin och begrepp i referensarkitektur

för IAM [IAM-RA]. Referensarkitekturen för IAM [IAM-RA] beskriver standarder och krav inom IAM. De kraven reglerar hur skyddsmekanismerna ska realiseras med avseende på tillämpade standarder för säkerhet. Observera att skyddsmekanismer i arkitektur för telemedicin enbart förhåller sig till patienten/den enskilde i rollen Användare och att IAM-termen e-tjänst i detta sammanhang därför syftar på byggblocken med patienten/den enskilde som användare: *Applikation för datafångst* och tjänst med *Eget konto*.

[Version 1.0 av [IAM-RA] täcker inte patient/individ-initierade flöden på ett sätt som motsvarar kraven för telemedicin. Målet är att nästa version av [IAM-RA] ska täcka flöden med lös koppling mellan identifiering för utfärdande av åtkomstintyg och identifiering för åtkomst av e-tjänst (praxis i sociala medier). Likaså finns behov av att kunna ansluta en personlig enhet direkt till en Säkerhetstjänsten för API. Idag ställer [IAM-RA] krav på att e-tjänsten/appen ska levereras med en egen server (”back-end”) för att få ansluta till Säkerhetstjänst för ett API.

Figuren visar en preliminär version av en sådan vy ur [IAM-RA].]

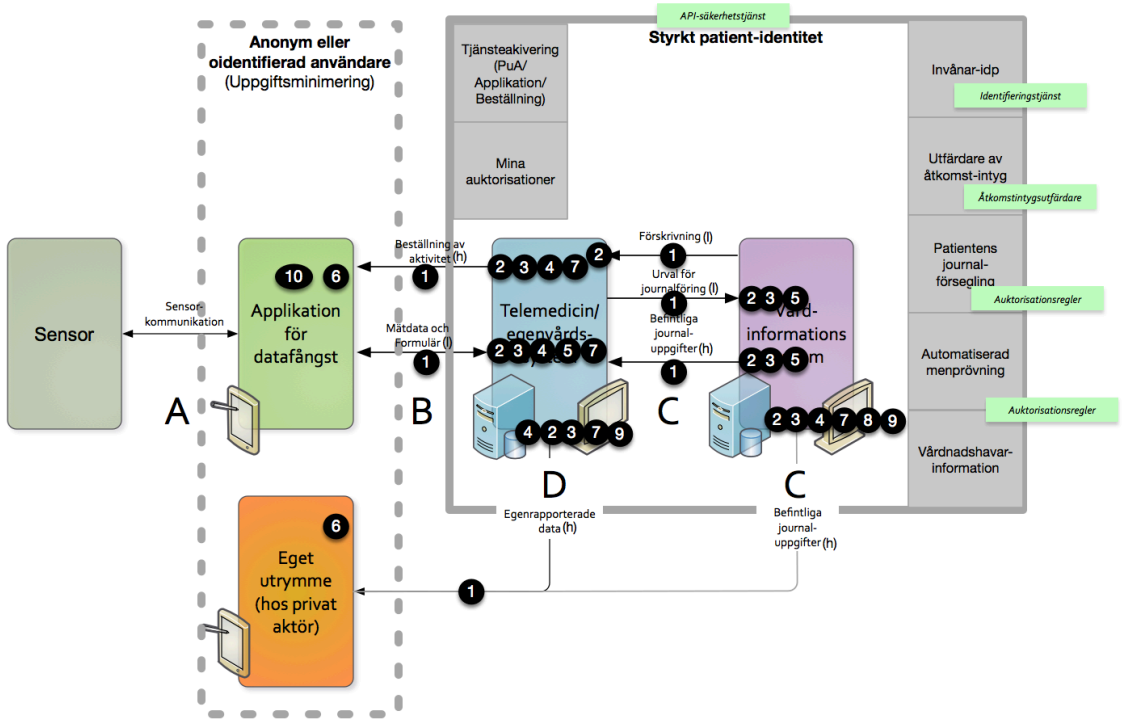
Siffrorna i Figur 19 refererar till kraven i avsnitt 9.2. Siffrornas placering indikerar vilka komponenter i [IAM-RA] som realiserar respektive krav.



Figur 19 Informationssäkerhetskrav i relation till IAM referensarkitektur (Att göra: -uppdatera [IAM_RA] och lägg in korrekt figur)

Liksom Figur 19 illustrerar Figur 20 relationen mellan skyddskraven, byggblocken i referensarkitektur men med referensarkitekturen för telemedicin som utgångspunkt. Gröna etiketter refererar begrepp ur [IAM-RA]. Grå rektanglar symboliserar de tekniska komponenter

som samverkar i realiseringen av skyddskraven. De tekniska komponenterna beskrivs i detalj i efterföljande avsnitt.



Figur 20 Referensarkitekturen i förhållande till [IAM-RA]

10.1.1 Komponenten Tjänsteaktivering

Komponenten tjänsteaktivering håller masterdata om de *Applikationer för datafångst* och tjänster för *Eget utrymme* som godkänts för anslutning till *Telemedicin/egenvårdssystem*. Dessa masterdata består åtminstone av följande element:

- Produktbeskrivning för applikationen
- Utfärdande organisation (organisationsnummer, kontaktuppgifter)
- Applikationsnyckel för API-anrop
- Applikationens publika certifikat (för autentisering och kryptering av kanal för informationsutbyte)
- Godkända informationsutbyten (med mappning till OAUTH-scopes [IAM-RA]) – d.v.s. de informationsutbytenen som användaren kan välja att aktivera och vad som är maximal längd på aktiveringstid för respektive informationsutbyte)
- Personuppgiftsansvariga vårdgivare som accepterar informationsutbyte med applikationen (i praktiken de som har biträdesavtal med leverantören av applikationen)
- Tidpunkt för godkännandet

Informationen konsumeras av Komponenten Tjänsteaktivering och Komponenten Mina auktorisationer.

Informationen administreras av det organ som ansvarar den process som godkänner nya applikationer för datafångst. Komponenten behandlar inte patientuppgifter. Den kan komma att behandla personuppgifter i det fall medarbetare hos utfärdande applikation registreras, eller om administratörers personuppgifter lagras för spårbarhet avseende ändringar i lagrade masterdata.

10.1.2 Komponenten Mina auktorisationer

”Mina auktorisationer” är den webbapplikation där användaren (den enskilde) av en e-tjänst aktiverar (auktoriserar) informationsutbyten enligt B, C eller D-gränssnitten när de begärs av en e-tjänst [IAM-RA]. Det är i denna webbapplikation som en anonym eller oidentifierad användare avkrävs en styrkt personidentitet, som en förutsättning för att tilldela rättigheter till en e-tjänst avseende utbyte av personuppgifter med anslutna *Telemedicin/egenvårdssystem* (gränssnitt B och D) och *Vårdinformationssystem* (gränssnitt C).

Komponenten behandlar åtminstone följande personuppgifter:

- Den enskildes personidentitet
- Applikationsnyckel (identifierar masterdata i *Komponenten Tjänsteaktivering*) för den applikation den enskilde valt att aktivera för informationsutbyte
- Rättigheterna till informationsutbyte (”scopes”) som den enskilde aktiverat för e-tjänsten (hela eller delar av applikationens godkända utbud av informationsutbyten, enligt masterdata i *Komponenten Tjänsteaktivering)*
- De personuppgiftsansvariga vårdgivare som aktiveringen gäller (alla eller en delmängd av dem som kan aktiveras enligt masterdata i *Komponenten Tjänsteaktivering*)
- Auktorisationens giltighetstid inom ramen för maximal giltighetstid enligt masterdata i *Komponenten Tjänsteaktivering*

Det är också i denna webbapplikation som den enskilde kan se en förteckning över sina aktiverade informationsutbyten. Vyn med förteckningen ska ge den enskilde möjlighet att avaktivera (återkalla) enskilda e-tjänsters tilldelade rättigheter till informationsutbyte. Denna vy bör täcka alla vårdgivare. Det är viktigt för att den enskilde ska känna trygghet i att det finns en säker källa till information om hens samtliga godkännanden.

Komponenten lagrar inga personuppgifter. Den är den enskildes användargränssnitt till *Komponenten Utfärdare av åtkomstintyg*. Ansvaret för hanteringen av personuppgifterna ligger hos den enskildes folkbokföringslandsting.

10.1.3 Komponenten Utfärdare av åtkomstintyg

Komponenten beskrivs i generella termer i [IAM_RA]: ”Åtkomstintygsutfärdare”. I Referensarkitekturen för telemedicin är komponentens roll avgränsad till följande ansvarsområden:

- Att ge den enskilde möjlighet utfärda åtkomstintyg åt de e-tjänster som utbyta patientbunden information genom de FHIR-API:er som *Komponenten API-säkerhetstjänst* publicerar

- Att vara ”back-end” till Komponenten Mina auktorisationer
- Att realisera rollen ”Auth-server” i OAUTH-protokollet [IAM-RA]

Komponenten tillgängliggör ett API för Komponenten Mina auktorisationer och konsumerar det API som tillgängliggörs av Komponenten Tjänsteaktivering.

Komponenten behandlar och lagrar åtminstone följande personuppgifter:

- Den enskildes personidentitet
- Applikationsnyckel (identifierar masterdata i *Komponenten Tjänsteaktivering*) för den applikation den enskilde valt att aktivera för informationsutbyte
- Rättigheterna till informationsutbyte (”scopes”) som den enskilde aktiverat för e-tjänsten (hela eller delar av applikationens godkända utbud av informationsutbyten, enligt masterdata i *Komponenten Tjänsteaktivering)*
- De personuppgiftsansvariga vårdgivare som aktiveringen gäller (alla eller en delmängd av dem som kan aktiveras enligt masterdata i *Komponenten Tjänsteaktivering*)
- Auktorisationens giltighetstid. Den begränsas av maximal giltighetstid enligt masterdata i *Komponenten Tjänsteaktivering*
- Det åtkomstintyg (OAUTH) som identifierar den enskildes åtkomstbeslut. Intyget identifieras av personidentitet, rättigheter, PUA och applikationsnyckel.
- Eventuell tidpunkt för återkallande av intyget

Folkbokföringslandstinget ansvarar för lagring och hanteringen av personuppgifter.

10.1.4 Komponenten Patientens journalförsegling

Information som individen (genom s.k. försegling) eller vårdgivaren (genom menprövning) beslutat undanta från individens åtkomst p.g.a. vanmaktssituation ska filtreras bort som del av informationsöverföringen. Uppgifter om att vissa patientuppgifter ska undanhållas från alla e-tjänster för invånare administreras och lagras i ett nationellt register. Registrets innehåll används av *Komponenten API-säkerhetstjänst* för att filtrera information från källsystem innan den når invånarens e-tjänster.

Folkbokföringslandstinget ansvarar för lagring och hanteringen av personuppgifter.

10.1.5 Komponenten Automatiserad menprövning

Alla tjänstekontrakt [T-boken] som syftar till att källsystem [T-boken] tillgängliggör befintliga journaluppgifter för användning i e-tjänster med den enskilde som användare, ska ställa krav på att tjänsteproducenten [T-boken] automatiskt menprövar efterfrågad information.
Tjänstekontrakten ska ha ett fält i svarsmeddelandet där utfallet av menprövningen redovisas.
Den utförande komponenten är i detta fall respektive tjänsteproducent.

Komponenten API-säkerhetstjänst använder information om utfallet av menprövningen till att filtrera bort poster med negativt utfall.

Personuppgiftsansvarig vårdgivare ansvarar för att den automatiserade menprövningen är realiserad i de tjänsteproducenter som tillgängliggör journaluppgifter.

10.1.6 Komponenten API-säkerhetstjänst

En API-säkerhetstjänst [IAM-RA] hanterar i detta sammanhang informationsutbyte mellan den enskildes applikationer och bakomliggande *Telemedicin/egenvårdssystem* och/eller *Vårdinformationssystem.* API-säkerhetstjänsten publicerar med andra ord API:er för de informationsutbyten i gränssnitt B, C och D som rör utbytet mellan den enskildes tjänster (E-tjänster enligt [IAM-RA]) och *Telemedicin/egenvårdssystem* och/eller *Vårdinformationssystem.*

Komponentens roll avgränsad till följande ansvarsområden:

- Att realisera rollen ”Resource server” i OAUTH-protokollet [IAM-RA]
- Att ta emot API-anrop (RIV-TA: ”Begäran”)
- Att agera FHIR-server i förhållande till anropande applikation
- Att validera att API-anropets åtkomstintyg är giltigt i tid och utfärdat för anropande E-tjänst (om e-tjänsten har en server sker valideringen mot SSL-förbindelsen klient-certifikat)
- Att vidareförmedla API-anropet till underliggande källsystem eller tjänsteplattform [T-boken]
- Att avgränsa API-anropet till de vårdgivare som omfattas av åtkomstintyget
- Att berika inkommande anrop med den enskildes personidentitet och att ta bort den enskildes personidentitet och övriga identifierande uppgifter från data som förmedlas tillbaka till anropande klient (svaret)
- Att filtrera bort information baserat på patientens förseglingsregler
- Att filtrera bort information som saknar information om menprövning eller som har negativt resultat från menprövning

Komponenten förlitar sig på PAI-tjänster från andra komponenter enligt Tabell 1

Tabell 6 - API-säkerhetstjänstens beroenden till andra komponenters API:er

Behov	Komponent	Bidrag
Översätta klientens applikationsidentitet till dess publika certifikat	Komponenten Tjänsteaktivering	Ger tillgång till applikationens publika certifikat baserat på applikationsidentitet.

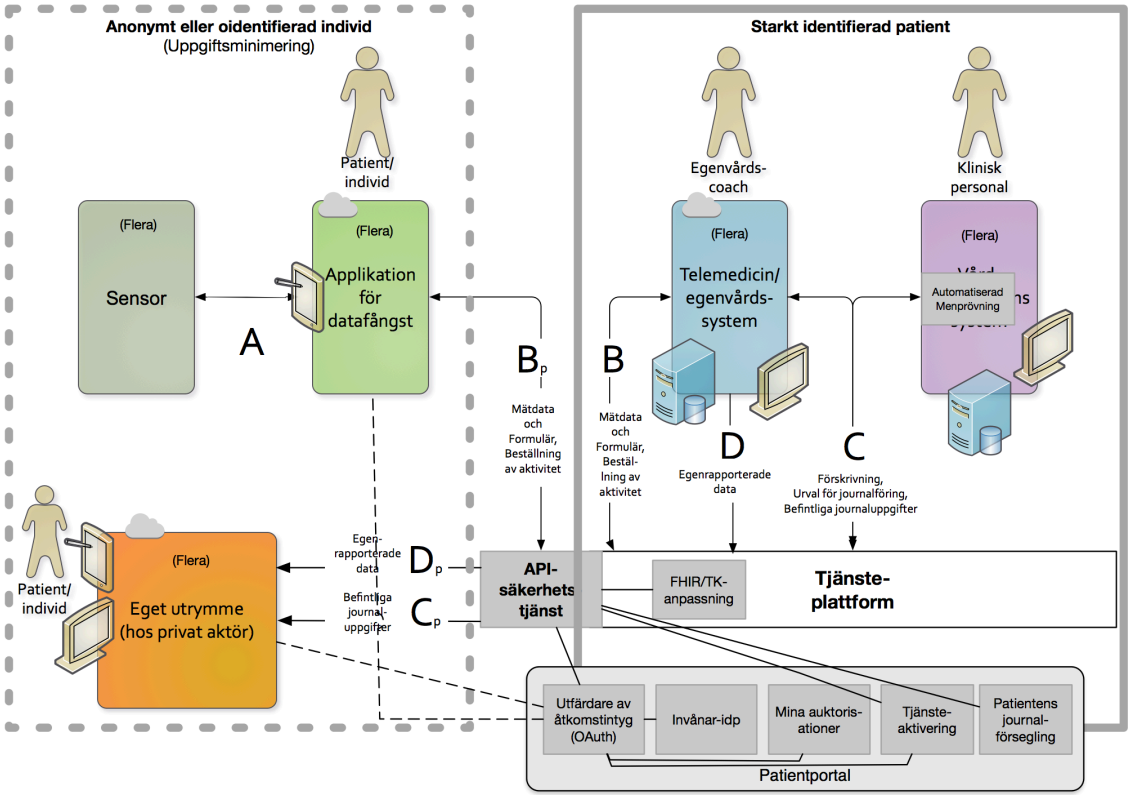
Validera att intyget är giltigt	Komponenten Utfärdare av åtkomstintyg	Ger tillgång till intygets giltighetstid
Validera att intyget är utställt för e-tjänsten	Komponenten Utfärdare av åtkomstintyg	Ger tillgång till åtkomstintygets applikationsidentitet
Validera att e-tjänsten är auktoriserad för aktuellt anrop	Komponenten Utfärdare av åtkomstintyg	Ger tillgång till åtkomstintygets rättigheter (”scopes”)
Begränsa anropet till aktuella vårdgivare	Komponenten Utfärdare av åtkomstintyg	Ger tillgång till åtkomstintygets auktoriserade vårdgivare
Berika anropet med patientens personidentitet	Komponenten Utfärdare av åtkomstintyg	Ger tillgång till åtkomstintygets personidentifierare
Undanhålla förseglade uppgifter	Komponenten Patientens journalförsegling	Ger tillgång till patientens förseglingsuppgifter
Undanhåll uppgifter med negativ menprövning	Komponenten Automatiserad menprövning hos respektive tjänsteproducent	Markerar utfall av menprövning för varje tillgängliggjord journalpost

Folkbokföringslandstinget ansvarar för hanteringen av personuppgifter.

10.1.7 Realisering i nationell samverkansarkitektur

Figur 21 illustrerar hur skyddsmekanismernas komponenter kan realiseras i referensarkitektur för nationell samverkan [T-boken]. De informationsgränssnitt som tillgängliggörs i API-säkerhetstjänsten uppträder i två versioner: med och utan personidentitet (och andra identifierande personuppgifter). Postfix ”p” markerar versionen utan personidentifierande uppgifter.

Såväl tjänsteplattform som patientportal kan vara regionala eller nationella. Komponenten *Patientens journalförsegling* behöver i samtliga fall kunna tillgängliggöra förseglingsinformation från en nationell källa. Det gäller även komponenten *Mina auktorisationer*.



Figur 21 Realisering i nationell samverkansarkitektur

10.2 Aggregerande tjänster och dubbletter

[T-boken] beskriver hur engagemangsindex och aggregerande tjänster används för att i ”runtime” skapa en nationell vy av patientens information, oavsett hur källinformationen förvaltas inom respektive vårdgivare eller huvudman. När det gäller telemedicin uppstår frågeställning om hur dubletter kan undvikas när en och samma insamlad uppgift förkommer i såväl ett *Telemedicin/egenvårdssystem* som ett *Vårdinformationssystem*. Den situationen kan uppstå under en pågående behandling där kliniska beslut dokumenterats. Efter att behandlingen avslutats gallras uppgifterna i *Telemedicin/egenvårdssystemet*. Men under mellantillståndet kan dubbletter uppstå i en aggregerande tjänst för mätvärden eller formulär.

Därför ska tjänsteproducenter för *Telemedicin/egenvårdsystem* enbart returnera formulär och mätvärden som ännu inte journalförts.

10.3 Specifika krav

Den tekniska arkitekturen beskriver tekniska lösningsmönster för gemensamma komponenter (infrastrukturkomponenter). Kraven är därför en integrerad del av respektive komponents beskrivning.