ANSVARSFÖRHÅLLANDEN I DIGITALA TJÄNSTER, MED ELLER UTAN HÄLSOKONTO

Jakob Dumky
2020-12-09

COMPLICITY

Innehålll

1 Inledning

Regeringens vision är att Sverige ska vara bäst i världen på att använda e-hälsans möjligheter år 2025 och det syns en kraftig ökning av digitala hälsotjänster både på forskningsområdet och på den kommersiella marknaden. Den offentligt finansierade vården försöker komma ikapp men brottas med gamla system och tröga strukturer.

Samtidigt står svensk hälso- och sjukvård inför stora utmaningar med en åldrande och ökande befolkning samtidigt som pensionsavgångar och sparbeting gör att personalmängden minskar. Färre vård- och omsorgsanställda ska helt enkelt kunna hjälpa fler individer. För att det ska fungera krävs effektiviseringar inom vården och att individen gör mer själva för sin egen och sina närståendes vård. Självhjälp, egenvård och digitala vårdkontakter kommer därför att bli en allt viktigare del av hälso- och sjukvården.

Just nu pågår en digital omställning i hela samhället som förändrar vanor, behov och förväntningar. Allt fler digitala tjänster används och genererar data som avspeglar användarens hälsa och levnadsvanor. Denna data skulle kunna spela en viktig roll i effektiviseringen av hälso- och sjukvården. Samtidigt kan den data som genereras inom den etablerade hälso- och sjukvården spela stor roll i individens användande av hälsorelaterade digitala tjänster.

Många applikationer och molntjänster tjänar som gränssnitt mellan patient och vårdgivare. Det kan röra sig om hälsoenkäter som fylls i hemmet före ett fysiskt vårdbesök, provtagning och analys i hemmet, monitorering med hjälp av sensorer, grafiska beskrivningar av smärta, alkomätare etcetera Tjänsterna ger ökad självständighet för invånare samtidigt som vårdgivare kan arbeta mer effektivt och med högre tillgänglighet och kvalitet. Tjänsterna är också bra på att strukturera data så att de på ett systematiskt sätt kan föras in i patientjournalen och i övrigt användas för uppföljning och utvärdering.

Varianterna av lösningar på det trepartsförhållande som uppstår mellan tillverkare, vårdgivare och individ är många, exempelvis: konton erbjuds individer av vårdgivare eller finansieras av vårdgivare; konton vidareförmedlar data till vårdgivare från kontot eller ger vårdgivare direktåtkomst till

kontot; vårdgivare eller tillverkare tillhandahåller sensorer till patienten; vårdgivaren finansierar sensorerna.

Det finns många fördelar för alla parter med denna typ av lösningar. Individen förfogar över samma data som vårdgivaren. När en vårdepisod är avslutad har individen kvar sina data och kan fortsätta använda kontot för egen monitorering av sin hälsa, kanske byta vårdgivare och lämna in insamlade data till en ny vårdgivare för en second opinion. Tillverkaren förfogar likaså över identifierbara data från individens konto för sina egna behov, till exempel utveckling av tjänsten (med stöd av individens samtycke). Vårdgivaren spar tid genom automatiserad övervakning av individen eller distanssjukvård samt förfogar över nödvändiga data för vård och behandling. Vid användning av tjänsten uppstår en situation där flera parter behandlar samma personuppgifter inom ramarna för tjänsten. Ansvar för personuppgifterna måste fastställas för att ge möjlighet att uppfylla krav i GDPR.

Något gemensamt personuppgiftsansvar menar vi inte föreligger. Ändamålen med behandlingarna är inte gemensamma; vårdgivaren behandlar personuppgifter för ändamålet hälso- och sjukvård och tillverkaren behandlar personuppgifter i enlighet med tjänstens avsedda användning, till exempel självhjälp eller egenvård.[1] Det är inte en situation där ändamålen är odelbara, det vill säga oupplösligt kopplade till varandra. Det finns alltid ett val för vårdgivaren att själv tillhandahålla en digital tjänst för egenvård som hälso- och sjukvård och för en tillverkare ett val att erbjuda en tjänst för självhjälp med samma syfte som egenvård. Vårdgivaren och tillverkaren bestämmer inte heller över samma medel, särskilt inte om olika delar av tjänsten och tillhörande utrustning tillhandahålls av båda aktörerna.

Vårdgivaren är enligt patientdatalagen (2008:355; PDL) personuppgiftsansvarig för vårdpersonalens behandling av personuppgifter för syftet sjukvård. Tillverkaren är enligt GDPR personuppgiftsansvarig för behandlingen av

[1] Av Socialstyrelsens föreskrifter (SOSFS 2009:6) om egenvård framgår att egenvård inte är hälso- och sjukvård enligt hälso- och sjukvårdslagen. Därmed är inte patientdatalagen tillämplig på eventuell databehandling som sker inom ramen för egenvård. Egenvård ligger utanför hälso- och sjukvårdens ansvar med undantag för egenvårdsbedömning, planering och uppföljning av egenvårdsbeslutet.

personuppgifter när produktens avsedda användning riktas direkt till invånaren.

Men det finns risker som kan rubba detta ansvarsförhållande. Ju mer aktiv roll vårdgivare tar för behandlingen av personuppgifter i ett hälsokonto, desto större är dock risken att vårdgivare får ett ”helhetsansvar” för den behandlingen. Tillverkare riskerar då att utge skadestånd till vårdgivaren för vårdskada som drabbat patient eftersom tjänsten – hälsokontot – har ett vårdsyfte, men tjänsten inte lever upp till vare sig patientsäkerhetslagens eller GDPR:s krav på säkerhet respektive riktighet i data. Det är tveksamt om en tillverkare kan avtala om ansvarsfrihet för sådan skada enligt avtalslagen (se 36 § avtalslagen om oskäliga avtalsvillkor) och GDPR (art. 82).

Tydlig rollfördelning inom eHälsa är till fördel för alla parter: konsumenter, tillverkare och vårdgivare. Det finns dock juridiska risker som både vårdgivare och tillverkare måste uppmärksamma. I denna framställning analyseras riskerna och olika lösningar övervägs för att undvika identifierade risker och låta tillverkare och vårdgivare samexistera i leveransen av digitala tjänster som innefattar hälsokonton. Just nu råder en inlåsningseffekt som gör att data inte kommer till användning i den utsträckning som skulle vara möjlig. Anledningen är avsaknad av etablerade affärsmodeller för både tillverkare och vårdgivare, vilket beror på ett osäkert rättsläge och oklara ansvarsförhållanden. I denna framställning försöker vi identifiera lösningar som skulle kunna låsa upp tillgången till data genom att analysera ansvar för data ur tre perspektiv: vårdgivarens, tillverkarens och individens.

Avsnitt två till fyra definierar vårdgivar-, tillverkar och individperspektivet. Avsnitt fem till tretton analyserar förhållanden, lagkrav, risker och möjligheter som sammantaget skapar underlag för de slutsatser som presenteras i avsnitt fjorton. Vill du som läsare bara förstå angreppssätt och krav som är lämpliga för olika parter räcker det med att läsa avsnitt fjorton. Är du dock intresserad av varför dessa krav är lämpliga bör du läsa hela dokumentet.

2 Vårdgivarperspektivet

2008 beslutade riksdagen om en ny registerförfattning för hälso- och sjukvården – patientdatalagen PDL). Lagen reglerar vårdgivares personuppgiftsansvar och behandling av personuppgifter i hälso- och sjukvården. Lagen är över tio år gammal och är i vissa delar i behov av en översyn för att kunna hålla jämna steg med digitaliseringen och Big Data inom hälso- och sjukvården.[2]

Styrkan hos PDL finns dock kvar. En vårdgivare, dvs. en aktör som yrkesmässigt erbjuder hälso- och sjukvård, t.ex. regioner och vårdbolag, får databehandla patientuppgifter inom sin egen organisation för en mängd olika ändamål som normalt faller inom kärnverksamheten och rättsliga förpliktelser enligt författning. Som exempel kan nämnas journalföring, upprättande av annan dokumentation som behövs i och för vården av patienten, uppföljning, utvärdering, kvalitetssäkring, statistik och egenkontroll (2 kap. 4 § PDL). Något samtycke behöver vårdgivaren inte inhämta från patienten. Samma data får användas av vårdgivaren ”sömlöst” mellan de olika ändamålen, vilket är en stor fördel för vårdgivare.

Om en vårdgivare vill behandla personuppgifter för andra ändamål än de som är tillåtna enligt PDL måste stöd sökas i annan författning. PDL erbjuder dock en möjlighet för en vårdgivare att lagligen behandla personuppgifter som inte är tillåten enligt lagen. Av PDL framgår nämligen att behandling av personuppgifter som inte är tillåten enligt lagen får ändå ske, om den enskilde lämnat ett uttryckligt samtycke till behandlingen (PDL 2 kap. 3 §). Enligt praxis får dock vårdgivare med stöd av ett sådant uttryckligt samtycke inte lämna ut eller ta del av uppgifter genom direktåtkomst som saknar stöd i lagen.[3]

En vårdgivare är, enligt PDL, personuppgiftsansvarig för den behandling av personuppgifter som vårdgivaren utför. I region och kommun är varje myndighet som bedriver hälso- och sjukvård personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför (PDL 2 kap. 6 §). Man behöver således inte fundera över vem som är personuppgiftsansvarig när en vårdgivare anlitar en

[2] Se bl.a. SOU 2014:23.
[3] Högsta förvaltningsdomstolens dom 2017-12-04, mål nr 3716-16.

tillverkare för att behandla dennes patientuppgifter – det är alltid vårdgivaren eftersom det är reglerat i PDL. Detta ansvar kan en vårdgivare inte avtala bort. Med personuppgiftsansvaret följer en skyldighet att säkerställa att behandlingen är laglig och att skydda personuppgifterna samt att tillmötesgå den registrerade, patienten, när denne åberopar sina rättigheter enligt PDL eller GDPR.

Data inom hälso- och sjukvården behöver också vara riktiga för att inte äventyra patientsäkerheten. Sådana krav ställs dock inte i PDL. Krav på kvalitet och patientsäkerhet i en vårdgivares verksamhet finns i andra författningar. Därutöver finns grundläggande dataskyddsprinciper stadgade i GDPR. En av dessa principer är att personuppgifter ska vara riktiga (art. 5.1 d). Kvalitetskrav på vårdens informationstillgångar finns också i hälso- och sjukvårdslagen (2017:30), patientsäkerhetslagen (2010:659) och lagen (1993:584) om medicintekniska produkter. Framställningen återkommer till dessa lagar.

Några av de större regionerna har ett tillfredsställande populationsunderlag för att kunna utföra analyser, prediktionsmodeller och beslutsunderlag med god kvalitet. I t.ex. Västra Götalandsregionen finns omkring 1,6 miljoner invånare. Många av dem är eller har varit patienter. Behövs däremot data från andra vårdgivare eller aktörer, t.ex. Socialstyrelsens hälsodataregister, uppstår problem. Patientuppgifter kan inte fritt flöda mellan vårdgivare, eller mellan vårdgivare och Socialstyrelsen. Det beror på att det råder en stark sekretess och tystnadsplikt för uppgifterna.

Bestämmelser om sekretess inom den allmänna hälso- och sjukvården (stat, region och kommun) finns i offentlighets- och sekretesslagen (2009:400). Tystnadsplikt för den enskilda hälso- och sjukvården finns i patientsäkerhetslagen. Utgångspunkten är att det råder sekretess och tystnadsplikt för patientuppgifter. Sekretessen är stark. Den som bryter mot rådande sekretess eller tystnadsplikt för uppgifter kan dömas till böter eller fängelse för brott mot tystnadsplikten. I vissa fall får en vårdgivare röja sådana uppgifter, t.ex. till Socialstyrelsens hälsodataregister. Då är det reglerat i lag. Men Socialstyrelsen får å andra sidan inte lämna ut hälsodatauppgifter till vårdgivare för användning i vården. Vidare får en vårdgivare röja en patients uppgifter för någon annan med patientens samtycke.

3 Tillverkarperspektivet

I denna framställning används medvetet inte begreppet leverantör för digitala tjänster inom eHälsa. Enligt Svenska Akademins ordlista menas med leverantör en person eller företag som (regelbundet) tillhandahåller viss vara till viss kund e.d. Begreppet säger ingenting om leverantörens ansvar och skyldigheter.

Eftersom denna framställning diskuterar ansvarsförhållanden för uppgifter i digitala tjänster inom hälso- och sjukvården, används i stället begreppet **tillverkare**. Begreppet är hämtat från produktsäkerhetslagstiftningen, i detta fall lagen om medicintekniska produkter. Med tillverkare avses i lagen den fysiska eller juridiska person som har ansvaret för utformningen, tillverkningen, paketeringen och märkningen av en produkt innan den av tillverkaren själv, eller av annan för tillverkarens räkning, släpps ut på marknaden som tillverkarens produkt.

Enligt den medicintekniska förordningen, MDR 2017/745, är en tillverkare ansvarig för säkerhet och prestanda i en medicinteknisk produkt som görs tillgänglig på marknaden. Ansvaret för säkerhet och prestanda inkluderar användningen av data inom ramen för tjänsten.

Tillverkaren formar tjänsterna för att möta användarens behov och itererar ofta fram lösningen för att först lösa användarens mest centrala problem för att sedan över tid hantera fler och bredare funktioner. I den iterativa processen är tillverkaren ofta beroende av den data som genereras genom användande av tjänsten då detta ger underlag för att förstå användarens beteende och behov.

En av de större utmaningarna som tillverkare av tjänster inom e-hälsa möter är hur affärsmodellen ska utformas. Affärsmodeller för digitala tjänster ofta förlitar sig på tillgången till data. Det är nämligen inte självklart att tillverkaren har tillgång till den data som genereras inom ramen för tjänsten. Tillverkaren tvingas ta höjd för detta vid utformningen av affärsmodell.

Tillverkarens tillgång till och ansvar för data i tjänsten skiljer sig beroende på vem tjänsten levereras till. Om tillverkarens

tjänst är avsedd för hälso- och sjukvård som bedrivs av vårdgivare, hanterar tillverkaren som regel personuppgifter i rollen som s.k. personuppgiftsbiträde. Ett personuppgiftsbiträde är en aktör som enligt GDPR behandlar personuppgifter för någon annans räkning.

Tillverkarens uppgift är att leverera tjänsten åt kund enligt villkor som framgår av avtal mellan parterna. Kunden, en vårdgivare, är regelmässigt personuppgiftsansvarig. Tillverkarens skyldighet att ”tillhandahålla tjänsten” inkluderar typiskt sett felsökning, test och support och annan administration. I alla dessa fallsituationer får tillverkarens personal, om så är nödvändigt, med kundens medgivande (som normalt kommer till uttryck i ett personuppgiftsbiträdesavtal), ta del av patientdata.

En tillverkare får dock inte använda data, inte ens metadata, för egna ändamål i rollen som personuppgiftsbiträde. Om den digitala tjänsten är ett medicinskt beslutsstöd, får alltså tillverkaren inte använda kundens (vårdgivarens) uppgifter för egna ändamål, t.ex. att vidareutveckla algoritmer eller AI i tjänsten eller som behövs för tjänsten. Det finns ingen sådan rätt vare sig i PDL, GDPR eller annan lagstiftning. Inget hindrar emellertid att tillverkaren på kundens uppdrag sambearbetar kundens data.

Riktar sig tjänsten direkt till individen innebär det att tillverkaren definierar ändamål och medel för den behandling av personuppgifter som sker i tjänsten, vilket innebär att tillverkaren enligt GDPR är personuppgiftsansvarig. Detta ger helt andra förutsättningar för tillverkaren att använda data i vidareutveckling av tjänsten och ger bredare möjligheter vid utveckling av affärsmodellen.

I dagsläget väljer många tillverkare av eHälsa att erbjuda **individer** egna konton, s.k. hälsokonton. Individen är i denna bilaterala kontext en konsument. Individen är inte patient. Sådana konton erbjuds med ett varierande utbud av tjänster och appar från tillverkaren själv eller tredjepartsleverantörer. Konsumentens egna hälsodata kan laddas upp till kontot i molnet, och delas med vänner och anhöriga.

En tillverkare får dock inte behandla sådana hälsorelaterade data i kontot med stöd av PDL. Tillverkaren är ingen vårdgivare. I stället måste tillverkaren falla tillbaka på

GDPR:s rättsliga grunder för databehandling och behandling av känsliga personuppgifter (art. 6.1 och 9.2). Som regel kan avtalet som ingås mellan parterna vid öppnande av konto läggas till grund för tillverkarens personuppgiftsbehandling. Vidare måste tillverkaren inhämta ett uttryckligt samtycke för att lagligen kunna behandla konsumentens hälsodata.

4 Individperspektivet

I takt med digitaliseringen av hälsorelaterade tjänster uppstår nya möjligheter för individen att delta i vården av sig själv. De nya verktygen som erbjuds kan samverka för att skapa en komplett bild av individens hälsotillstånd. Vitalparametrar kan korreleras med aktivitet och kostvanor för att ge en komplett hälsohistorik som borde vara relevant i en vårdsituation.

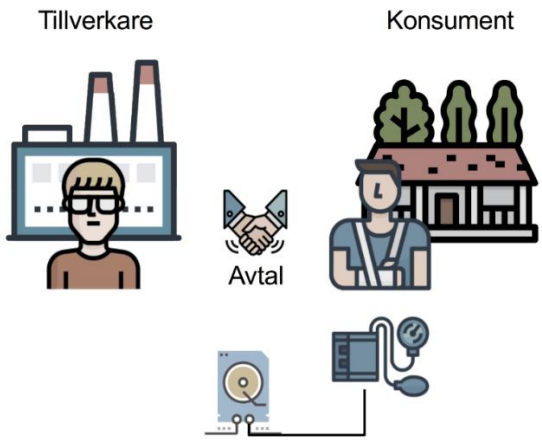
Individens tillgång till sin egna hälsodata ger nya förutsättningar för valfrihet och second opinion. Individens självbestämmande ökar och det blir lättare att delta i forskningen om sig själv samt att hitta andra som befinner sig i samma livssituation.

Individens hälsodata ska lagras någonstans. Detta sker lämpligen i de hälsokonton som tillhandahålls av tillverkaren direkt till individen. När individen lagrar sin data i ett hälsokonto existerar inte något biträdesförhållande mellan konsumenten och tillverkaren. Av GDPR följer att tillverkaren är personuppgiftsansvarig för uppgifterna. Det är tillverkaren som har kontroll över kontot och dess innehåll. Det s.k. privatundantaget i GDPR (artikel 2.2 c) är inte tillämplig när en tjänsteleverantör tillhandahåller en digital tjänst för konsumentbruk, oavsett om tjänsten är för privat bruk.

Konsumenternas rättigheter mot tillverkaren av hälsokontot regleras genom GDPR. Såvida databehandlingen sker med stöd av de rättsliga grunderna avtal och uttryckligt samtycke finns rätten att bli bortglömd. En återkallelse av samtycke är en automatisk begäran om radering. Rättar sig inte tillverkaren efter konsumentens begäran, kan konsumenten klaga hos Integritetsskyddsmyndigheten (tidigare Datainspektionen).

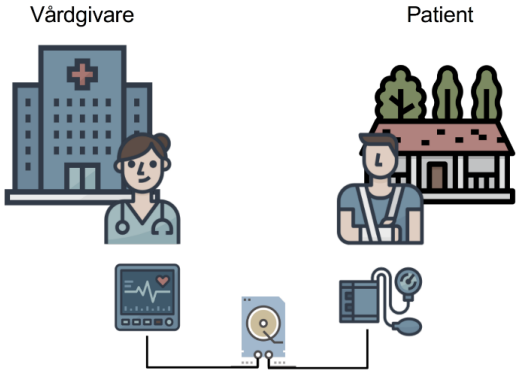
5 Konsumenttjänster vs. hälso- och sjukvård

När en molntjänst erbjuds direkt till en konsument för att användas av denne för att övervaka eller fatta egna beslut om sin hälsa utan inflytande av en vårdgivare, är det villkoren som definieras av tillverkaren av tjänsten och accepteras av konsumenten som styr det juridiska ansvaret för behandlingen av personuppgifter. Tjänsten kan eventuellt förskrivas av en vårdgivare, men om den enbart riktar sig till konsumentledet och personuppgifterna aldrig ska användas för hälso- och sjukvårdsändamål ska själva användningen betraktas som egenmonitorering eller självhjälp, dvs. en konsumenttjänst (se figur 1).



Figur 1. Tillverkaren av en tjänst tillhandahåller ett konto som används av patienten för egenmonitorering.

När däremot vårdgivare behandlar personuppgifter för att fatta beslut om diagnos eller behandlingsåtgärder rör det sig om hälso- och sjukvård enligt hälso- och sjukvårdslagen. Det spelar ingen roll vem som lämnar personuppgifterna till vårdgivaren. I sammanhanget är informationssäkerheten viktig för de uppgifter som används för hälso- och sjukvård. Vårdgivaren bär ett ansvar för riktigheten i och skyddet av personuppgifterna som används, se figur 2.

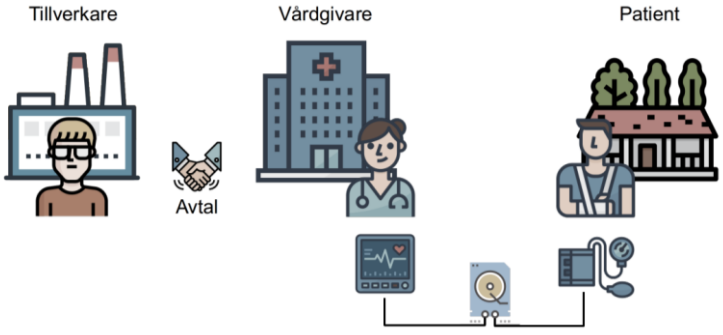


Figur 2. Vårdgivaren tar emot patientgenererade data för att fatta beslut om vård och behandling.

Det är när dessa två ”världar” möts som utmaningar uppstår. Vårdgivare kan inte ta ansvar för de beslut som tas av patienten själv utan ska ta ansvar för de beslut som fattas av hälso- och sjukvårdpersonalen. Vårdgivare kan inte heller tillåta att en tredje part kontrollerar informationen som används för hälso- och sjukvård inom dess organisation. En vårdgivare är alltid personuppgiftsansvarig för behandlingen av personuppgifter inom ramen för de tjänster som vårdgivaren levererar.

6 Vårdgivaransvar inte alltid ändamålsenligt

Vårdgivaransvar för ett hälsokonto kan fungera i de fall där tillverkarens ambition är att tillhandahålla en digital tjänst som enbart ska användas i relationen mellan vårdgivare och patient, men inte för andra syften som ligger utanför hälso- och sjukvård, såsom individers egen monitorering av hälsa eller egenvård enligt beslut av en vårdgivare (se figur 3).



Figur 3. Vårdgivaren tillhandahåller en tjänst till patient i syfte att tillhandahålla hälso- och sjukvård.

Annorlunda förhåller det sig om tillverkaren i första hand riktar sina tjänster till konsumentmarknaden. Det finns flera skäl till att tillverkaren erbjuder konsumenter hälsokonton i kombination med en produkt. Förutom att främja en egen produkt, till exempel GPS- och pulsklocka, elektroniska vågar, blodtrycksmanschetter eller alkomätare, kan tillverkaren ha ambitionen att skapa en egen relation och ”community” med sina konsumenter (se figur 1).

Tillverkaren har vidare behov av att förfoga över data i ett hälsokonto för egna syften utanför rollen som leverantör åt en vårdgivare. Data kan användas för att utveckla funktioner som ger individuella hälsoråd till kontoinnehavaren och för att utveckla AI. Självklart krävs konsumentens medgivande (samtycke), men när syftet med sådan avancerad databehandling handlar om att göra tjänsten smartare torde få konsumenter neka till sådan användning.

Att vårdgivaren lämnar instruktioner till patienten för egenvård innebär inte med automatik att vårdgivaren är personuppgiftsansvarig för behandlingen av personuppgifter i hjälpmedlet. När förskrivaren fattar sitt egenvårdsbeslut är denne enligt Socialstyrelsens egenvårdsföreskrifter (SOSFS 2009:6) enbart ansvarig för egenvårdsbedömningen, planeringen och uppföljningen av egenvården (1 kap. 2 §). Egenvården som patienten utför med hjälp av hjälpmedlet, t.ex. en digital tjänst eller utrustning, är enligt Socialstyrelsens föreskrifter inte hälso- och sjukvård (2 kap. 1 §). Av PDL framgår att en vårdgivare endast är personuppgiftsansvarig för den behandling som vårdgivaren utför, dvs. hälso- och sjukvård. I en region och en kommun är enligt PDL varje myndighet som bedriver hälso- och sjukvård personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför (2 kap. 6 §).

En vårdgivare är således personuppgiftsansvarig för behandling av personuppgifter för ändamålet ”hälso- och sjukvård”. Konsekvensen av ett egenvårdvårdsbeslut är att PDL inte är tillämplig på en vårdgivares behandling av personuppgifter, t.ex. en hälsodagbok som förs av en invånare i vårdgivarens e-tjänst utan en koppling till hälso- och sjukvård. För sådan behandling av personuppgifter måste vårdgivaren inhämta den enskildes samtycke för att kunna hävda en tillåten behandling av personuppgifter. Vårdgivaren får endast utan stöd av samtycke behandla personuppgifter

för de delar av egenvårdsbeslutet som vårdgivaren är ansvarig för. Det är endast vårdgivarens bedömning, planering och uppföljning som är att betrakta som hälso- och sjukvård. Den egenvård som den enskilde utför själv, eller med hjälp av någon annan, räknas inte som hälso- och sjukvård och omfattas därför inte av hälso- och sjukvårdslagstiftningen och därmed inte av patientdatalagen.

För vårdgivare är det inte självklart att axla ett ansvar för ett hälsokonto som kanske rymmer fler syften än bara hälso- och sjukvård. Ett uttryckligt samtycke krävs av patienten i dessa fall (2 kap. 3 § PDL). Samtycken kräver en administration, och de kan alltid återkallas. Att behandla en före detta patients personuppgifter när en vårdepisod har upphört är också en problematisk fråga för en vårdgivare. Särskilt om uppgifterna i hälsokontot inte utgör journalhandlingar. En konflikt kan uppstå mellan vårdgivarens skyldighet att gallra personuppgifter som inte längre behövs för verksamheten enligt GDPR:s dataskyddsprinciper (art. 5) och den före detta patientens behov av livslång åtkomst. Befinner sig tillverkaren i ett annat EU-medlemsland, eller i ett tredje land, försvårar det betydligt vårdgivarens möjligheter att utöva sitt juridiska ansvar för dataskyddet och sekretesskyddet i hälsokontot.

7 Medicinska syften eller sjukvård

Det erinras att hälso- och sjukvård och medicinskt syfte inte nödvändigtvis är samma sak. En produkt kan ha ett medicinskt syfte att registrera glukosvärden för att läggas till grund för dosering av insulin och planering av kost av patienten själv. Samma data kan dock vara av intresse för en vårdgivare i ett senare skede för att vårda patienten eller fatta beslut om ändrad egenvårdplan dvs. användas för hälso- och sjukvård.

Den som specificerar medicinskt syfte och användning av en produkt som sätts på marknaden är enligt medicintekniska förordningen, MDR 2017/745, tillverkare av produkten. Tillverkare är ansvariga för produktens prestanda och säkerhet. Det blir således viktigt att hälso- och sjukvården enbart använder produkten för de ändamål som specificerats och kommunicerats av tillverkare. Vårdgivare riskerar annars att ta på sig tillverkaransvar för produkten. Likaså är det viktigt för tillverkare att vara tydliga med avsedd användning

då det styr användningsområdet, både för konsumenten och sjukvården.

När konsumentgenererade data ska användas i en vårdgivares utövande av hälso- och sjukvård för en enskild patient är det viktigt att klargöra ansvaret för lämpligheten i att använda data för hälso- och sjukvårdsändamål. Detta görs genom att tillverkaren specificerar en avsedd användning som inkluderar medicinskt beslutsfattande i vården och CE-märker tjänsten som en medicinteknisk produkt. Genom att göra detta ansvarar tillverkaren för lämpligheten i att använda genererade data för kliniska ändamål och behöver således validera riktigheten fram till den punkt där det lämnas över till vårdgivaren.

8 Konsumentdata för klinisk användning

Det finns en tydlig trend mot självmonitorering av egen eller familjens hälsa inom ramen för privatlivet utan inblandning av vårdgivare – till dess sjukdomar, skador och smärta kräver en vårdgivarkontakt. Konsumenten sitter då i praktiken på värdefulla data som kan vara av intresse för en vårdgivare. Det är dock inte helt oproblematiskt att ge vårdpersonal tillgång till dessa uppgifter.

Enligt PDL är en vårdgivare personuppgiftsansvarig för den behandling av personuppgifter som vårdgivaren utför. I regioner och kommuner är varje myndighet som bedriver hälso- och sjukvård personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför (2 kap. 6 § PDL).

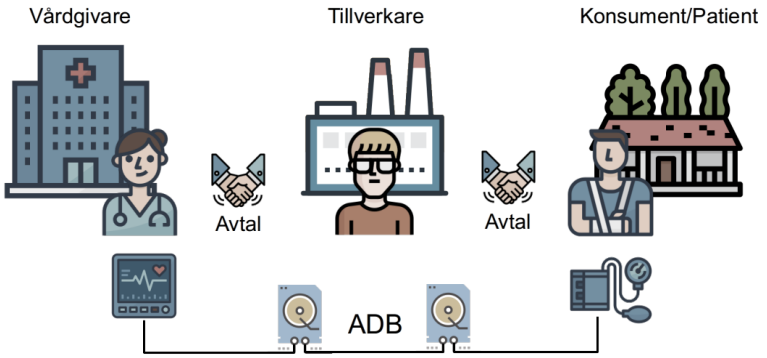
Vårdgivaren riskerar således att bli personuppgiftsansvarig för all behandling som sker i den digitala tjänsten. Den risken är påtaglig om vårdgivare har direktåtkomst till uppgifter om patient i hälsokontot. Detta gäller särskilt om uppgifterna som används för hälso- och sjukvård aldrig hamnar i vårdgivarens förvar. Det gäller således för vårdgivare att hitta andra sätt än genom direktåtkomst för att ta del av personuppgifter i ett hälsokonto som en individ förfogar över och som tillhandahålls av en tillverkare.

Om en behandling av personuppgifter är otillåten, måste ansvar utkrävas av någon, t.ex. vårdgivares direktåtkomst till en individs hälsokonto hos en tillverkare som är

personuppgiftsansvarig för kontot Personuppgiftsansvaret är styrande för vem som ska ställas till svars. Det ligger i farans riktning att det är vårdgivaren som bär ansvaret för den otillåtna direktåtkomsten, såvida inte vårdgivaren anses därigenom även ansvara för behandlingen av personuppgifter i hälsokontot.

9 Vårdgivarens egen lagringsyta

För att minimera risken för ett helhetsansvar vad gäller vårdgivarens personuppgiftsansvar för digitala tjänster som är avsedda för egenvård eller självhjälp behöver vårdgivaren säkerställa en egen lagring av de personuppgifter som ska behandlas av hälso- och sjukvårdspersonal. Detta kan åstadkommas genom tjänsten i sig eller genom en av vårdgivaren anvisad lagringsyta (se figur 4).



Figur 4. Vårdgivaren ska säkerställa att patientuppgifter lagras i en separat logisk lagringsyta skiljt från konsumentens hälsokonto. Saknas sådan lagringsyta i lösningen ligger det i farans riktning att vårdgivaren är personuppgiftsansvarig för den digitala tjänsten inklusive hälsokonto i stället för tillverkaren.

10 ADB-utlämnande istället för direktåtkomst

Ett sätt att undvika osäkerhet om en vårdgivares direktåtkomst är laglig eller inte är att lämna ut uppgifter via ADB-utlämnande. Ett ADB-utlämnande är en automatiserad behandling där data kopieras mellan två system.

Om en vårdgivare avser att lämna ut journaluppgifter till en patient (eller för den delen en före detta patient), ska detta ske genom en menprövning av vårdgivaren. Menprövade uppgifter överförs till en teknisk lagring som inte förvaltas av vårdgivaren, varvid de i rättslig mening anses utlämnade till den mottagare som ”prenumererar” på uppgifterna, till

exempel ett personligt hälsokonto. Motsvarande förfarande gäller när en vårdgivare vill ta del av patientens uppgifter i ett hälsokonto.

ADB-utlämnande är en möjlig lösning för att skapa stringenta ansvarsförhållanden för vårdgivarens respektive tillverkarens behandling av personuppgifter, och därmed undvika att vårdgivaren bryter mot lagen eller får ett helhetsansvar för behandlingen av personuppgifter i ett hälsokonto när dessa kommuniceras med vårdgivaren.

Informationsutbyten genom ADB-utlämnande kräver att det finns en standardisering av dataformat och dataöverföring som avtalas mellan parterna. Krav på integration mellan lagringsytorna bör också fastställas både vad gäller teknik och organisatoriska förhållanden.
Detta åstadkoms lämpligen genom att tillverkaren specificerar ADB-utlämnandet som en del i den avsedda användningen för de IT-system som avses för att sedan säkerställa att de tekniska förutsättningar som krävs implementeras som en del i tillverkarens produkt.

Samma förfarande kan tillämpas både i integrerade system där en och samma tillverkare levererar både vårdgivarens och patientens lagringsyta eller när olika tillverkare samverkar i en leverans där den ena tillhandahåller vårdinformationssystemet och den andra det personliga hälsokontot.

11 Datadelningsavtal

Vid överföring av personuppgifter från en personuppgiftsansvarig till en annan kan det uppstå osäkerhet när personuppgiftsansvaret för överförda uppgifter övergår från den ena parten till den andra. Det är en viktig omständighet att det juridiska ansvaret är klart och tydligt, inte minst för individen vars uppgifter hanteras av de båda aktörerna. Är personuppgiftsansvaret otydligt, finns det en risk att individen vars uppgifter hanteras ”bollas” mellan de personuppgiftsansvariga för att de inte själva vet vem som är personuppgiftsansvarig.

En sådan situation föreligger när vårdgivare vill ta del av personuppgifter om en individ som finns i ett hälsokonto som en tillverkare erbjuder konsumenter. Tillverkaren är

personuppgiftsansvarig för behandlingen i hälsokontot (med stöd av samtycke), och vårdgivaren är personuppgiftsansvarig för sin behandling av mottagna uppgifter från kontot.

För att det inte ska uppstå osäkerhet vid vilken punkt i processen personuppgiftsansvaret övergår från den ena personuppgiftsansvarige till den andra, bör parterna träffa ett datadelningsavtal. Ett sådant avtals främsta syfte är att reglera när personuppgiftsansvaret övergår från den ena parten till den andra. I ett sådant avtal brukar också normalt regleras rutiner vid avvikelser i informationsöverföringen, kontaktuppgifter och skyddsåtgärder.

Ett brukligt förfarande för att reglera mer exakt när personuppgiftsansvaret övergår från en part till en annan är kvittenser från mottagande servrar. En kvittens från mottagande server innebär att mottagaren tagit över personuppgiftsansvaret. En utebliven kvittens eller en felaktig kvittens innebär att personuppgiftsansvaret för överförda uppgifter kvarstår hos avsändaren och aktiverar rutiner hos båda parter för att undersöka vad som gått fel i transaktionen.

12 Avsedd användning och CE-märkning

En produkt som inbegriper ett medicinskt syfte är en medicinteknisk produkt. Bestämmelser om medicintekniska produkter finns som tidigare nämnts i förordningen om medicintekniska produkter, MDR 2017/745.

Avgörande för om en produkt är en medicinteknisk produkt är tillverkarens avsedda användning och verkningsmekanismen med produkten, inte konstruktionen eller användaren. En medicinteknisk produkt har ett medicinskt syfte. Det har den om tillverkaren har specificerat och beskrivit produkten så att den kan anses ha något eller några av de syften som beskrivs i definitionen av en medicinteknisk produkt i förordningen. Även programvaror och digitala tjänster som har ett medicinskt syfte omfattas av det medicintekniska regelverket.

Av skäl 21 i förordningen om medicintekniska produkter framgår följande: ”*Det bör klargöras att det är viktigt att produkter som erbjuds en person i unionen via*

informationssamhällets tjänster[4] *enligt Europaparlamentets och rådets direktiv (EU) 2015/1535 samt produkter som används i samband med kommersiell verksamhet för att tillhandahålla en diagnostisk eller terapeutisk tjänst till personer i unionen uppfyller kraven i denna förordning när den berörda produkten släpps ut på marknaden eller tjänsten tillhandahålls i unionen*."

Tillverkaren av en tjänst som är en medicinteknisk produkt ska alltså utöver GDPR även uppfylla kraven i MDR.

Tillverkaren av en medicinteknisk produkt är ansvarig för produktens säkerhet, prestanda och användbarhet i relation till produktens avsedda användning. Ansvaret sträcker sig över hela produktens livstid och kan inte avtalas bort.

I en digital tjänst som är avsedd att utöver egenvård eller självhjälp leverera konsumentdata för användning inom hälso- och sjukvården måste alltså tillverkaren säkerställa att mekanismer finns på plats för att förebygga att uppgifterna obehörigen röjs, ändras, görs otillgängliga eller förstörs, och förebygga skadlig inverkan i övrigt på uppgifter och informationssystem. Det handlar om att skapa en sådan tillit till uppgifterna att en vårdgivare inte hyser någon rädsla för felaktiga diagnoser eller åtgärder baserade på felaktiga värden.

Det ligger i sakens natur att en digital tjänst som inkluderar ett hälsokonto för att främja hälso- och sjukvård får anses säker och tillförlitlig inom angivet användningsområde om den är CE-märkt enligt det medicintekniska regelverket.

13 Förhållandet mellan MDR, GDPR och PDL

GDPR är tillämplig på behandling av personuppgifter i medicintekniska produkter. Därutöver kan PDL vara tillämplig på sådan behandling om en vårdgivare använder sig av medicintekniska produkter för ändamålet hälso- och

[4] Med informationssamhällets tjänster avses varje aktivitet som sker online, med någon ekonomisk innebörd (prop. 2001/02:150 s. 1 och 19). Begreppet informationssamhällets tjänster kan också innefatta bland annat olika sociala medier, till exempel bloggar, internetforum, webbplatser för videoklipp, chattprogram och sociala nätverk. Även online spel och olika applikationer (appar) för smarta enheter kan omfattas av definitionen (prop. 2017/18:105 s. 68).

sjukvård. Rollerna som personuppgiftsansvarig eller personuppgiftsbiträde enligt GDPR mellan vårdgivare och tillverkare kan dock variera beroende på strukturen i samarbetet vid användning av medicintekniska produkter.

Det är viktigt att notera att bestämmelser om dataskydd och medicintekniska produkter är två separata regelverk och att beskrivna roller inte är harmoniserade. Att en tillverkare omfattas av skyldigheterna enligt förordningen om medicintekniska produkter innebär inte med automatik att samma tillverkare alltid ska betraktas som personuppgiftsansvarig enligt GDPR.

Enligt GDPR är dock den som bestämmer över ändamål och medel för behandlingen av personuppgifter personuppgiftsansvarig för behandlingen. Att bestämma över ändamålen innebär i de scenarier som tas upp i denna framställning att fatta beslut om att tillhandahålla möjligheten för invånaren att nyttja tjänsten. Det verkar då rimligt att det är den som upprättar en relation med invånaren som står för ändamålen med behandlingen.

Om CE-märkningen *inkluderar* insamling av uppgifter från konsumenter till ett hälsokonto och på vilket sätt i form av datafångst, dataformat, datakälla (s.k. wearables, till exempel klockor eller andra produkter), datalagring, skydd mot avsiktlig eller oavsiktlig datamanipulation, åtkomst för enskild individ, överföring till vårdgivare över öppet nät med mera, *minskar det vårdgivarens utrymme att påverka tillverkarens datainsamling och överföringen av data till vårdgivaren*. Detta innebär alltså att tillverkaren likställer det medicinska syftet med tjänsten och syftet med behandlingen av data. Tillverkaren blir då ansvarig för lämpligheten att använda data i tjänsten för det av tillverkaren definierade syftet.

För att tillverkaren ska kunna säkerställa lämpligheten i de data som behandlas måste tillverkaren validera tjänsten mot den specificerade avsedda användningen och syftet med behandling av data. Valideringen ska säkerställa den nytta som uppstår genom användning av tjänsten. Tillverkaren måste bland annat säkerställa att de data som behandlas och presenteras är relevanta och uppnår tillräckligt hög grad av riktighet i förhållande till den avsedda användningen.

CE-märkning av digitala tjänster för hälsokonton torde därmed reducera eller eliminera risken att en vårdgivare anses personuppgiftsansvarig för ett hälsokonto enligt nationell tillsynsmyndighet. Utrymmet för vårdgivaren att påverka hälsokontots användningsområde som databärare för bland annat hälso- och sjukvård är beskuret genom CE-märkningen. CE-märkningen snarare stärker tillverkarens personuppgiftsansvar genom att ändamålen med och medlen för personuppgiftsbehandlingen är ”låsta” i en dokumentation som ligger till grund för CE-märkningen.

I situationer där både en konsumentrelation mellan tillverkare och konsument samt en vårdrelation mellan vårdgivare och patient pågår inom samma tjänst behöver tillverkaren definiera överlämningspunkten där personuppgiftsansvaret övergår till vårdgivaren. Vårdgivare eller tillverkare ska säkerställa att vårdgivaren har sin egen logiska lagring av patientuppgifter (se figur 4).

Om avsedd användning enligt tillverkarens specifikation och kommunikation istället är att uteslutande främja en relation mellan vårdgivare och patient innebär det att vårdgivaren får anses styra över syfte och medel för personuppgiftsbehandlingen (se figur 3). Av det skälet är vårdgivares personuppgiftsansvar reglerad i PDL. Någon relation mellan tillverkare och patient finns inte i detta scenario. Vårdgivaren blir således personuppgiftsansvarig för den behandling som sker i tjänsten.

14 Sammanfattning och slutsatser

Frågeställningarna som presenteras i denna framställning måste både vårdgivare och tillverkare av tjänster som innefattar hälsokonton ta höjd för. Både vårdgivare och tillverkare har sina befogade anledningar till att ta kontrollen över de personuppgifter som behandlas inom respektive verksamhet. Detta gör att lösningar måste tas fram som möjliggör att dessa världar kan mötas.

Medicinska syften och ändamål med behandling av personuppgifter bör sammanstråla från ett tillverkarperspektiv. Tillverkaren bör ta ansvar för den behandling av personuppgifter som sker när tillverkaren riktar tjänster direkt till individen. När tillverkaren istället riktar tjänsten till en vårdgivare för att användas av

vårdgivaren i en patientrelation borde tillverkaren säkerställa att IT-systemet ger vårdgivaren förutsättning att ta ansvar för den personuppgiftsbehandling som sker inom vårdgivarens verksamhet.

Regelverken (MDR, GDPR och PDL) bygger på samma grunder vilket innebär att ansvar inte går att avtala bort utan styrs av syften. Det innebär att det är tillverkarens avsedda användning med en produkt som avgör av vem och hur den kan användas. Tillverkaren måste alltså utforma produkten så att vårdgivaren kan ta det ansvar för personuppgifter som vårdgivaren ska enligt lag; om så inte är fallet är produkten inte lämplig och borde således inte kunna sättas på marknaden. När tillverkaren riktar tjänster till en individ kommer tillverkarens personuppgiftsansvar styrkas av tjänstens avsedda användning om tjänstens säkerhet och prestanda påverkas av den data som behandlas.

Ska konsumentrelationen mellan tillverkare och individ samexistera med patientrelationen mellan vårdgivare och individ behöver utlämnande av information ske. Tillverkare av de produkter som används för behandlingen av personuppgifter måste då inkludera detta utlämnande som en del i den avsedda användningen för produkten.

Tillverkaren måste:

- Definiera avsedd användning för produkten och där inkludera ändamål och medel för behandling av personuppgifter.
- Utfärda deklaration om riskacceptans och kommunicera kvarstående risk vid eventuella överlämningspunkter av data till andra aktörer.
- Följa upp användningen av produkten inklusive behandling av personuppgifter när detta kan påverka säkerhet och prestanda i relation till produktens avsedda användning.

Tillverkaren av en tjänst som innefattar ett hälsokonto som riktas direkt till individen bestämmer över ändamål och medel för behandlingen av personuppgifter som utförs i syftet självhjälp och egenvård. Tillverkaren är därav personuppgiftsansvarig för denna behandling vilket följer av kraven i GDPR. I detta fall ska tillverkaren där så är tillämpbart:

- Tillhandahålla ett konto direkt till individen.

- Definiera avsedd användning och ett tydligt medicinskt syfte.
- Definiera hälso- och sjukvårdssyfte för data som ska användas av vårdpersonal.
- Säkerställa åtskild lagring av data för olika syften med olika personuppgiftsansvariga, antingen genom utlämnande av data till vårdgivare eller genom tekniskt separerad lagring av vårddata inom tjänsten.
- Utforma lösningar för utlämnande av data till vårdgivaren på andra sätt än direktåtkomst avseende personuppgifter avsedda för ändamålet egenvård och självhjälp.
- Validera data mot det medicinska syftet och den avsedda användningen i alla överlämningar från den digitala tjänsten/produkten, både maskinläsbara och grafiska gränssnitt.

Vårdgivare ska bestämma ändamål och medel för den behandling av personuppgifter som utförs för syften som inbegriper hälso- och sjukvård. Vårdgivaren är därav personuppgiftsansvarig för denna behandling vilket följer av kraven i PDL. Det innebär bland annat att vårdgivaren måste:

- Säkerställa att teknisk lagring av personuppgifter som behandlas av vårdpersonal, förvaltas och ägs av vårdgivaren eller, som alternativ, säkerställa att externa tjänster (som inte förvaltas av vårdgivaren) som av hälso- och sjukvårdspersonal används för behandling av personuppgifter har tekniska förutsättningar för att få in personuppgifterna i vårdgivarens förvar inom ramen för tjänsten.
- Säkerställa att de IT-system som används för att möjliggöra hälso- och sjukvård är CE-märkta med en tydlig definierad avsedd användning och en överlämning av data som är validerad för den definierade avsedda användningen till vårdgivaren.
- Definiera syftet för de IT-system som tas in för användning i vårdgivarens verksamhet.

I det fall en tillverkare av en tjänst som innefattar ett hälsokonto som inte riktas direkt till individen utan som tillhandahålls till en vårdgivare för att vårdgivaren ska tillhandahålla ett hälsokonto till individen bestämmer vårdgivaren över ändamål och medel för behandlingen av personuppgifter. Vårdgivaren är då personuppgiftsansvarig för behandlingen av personuppgifter, vilket följer av GDPR

och PDL i det fall vårdpersonalen behandlar personuppgifter i tjänsten genom elektronisk åtkomst. Det innebär bland annat att vårdgivaren där så är tillämpbart ska:

- Tillhandahålla ett konto till patienten.
- Säkerställa att de IT-system som används för att möjliggöra hälso- och sjukvård är CE-märkta med en tydlig definierad avsedd användning och att vårdgivaren har tekniska och organisatoriska förutsättningar att sätta IT-systemet inom sin egen kontrollsfär.
- Definiera syftet för de IT-system som tas in för användning i vårdgivarens verksamhet och säkerställa att dessa syften stämmer överens med det av tillverkaren specificerade syftet i tjänsten.

Jakob Dumky