Ekosystem för E-hälsa

En juridisk genomlysning av hemmonitorering i hälso- och sjukvården

www.regionostergotland.se

Region Östergötland

Titel:	Ekosystem för E-hälsa - En juridisk genomlysning av hemmonitorering i hälso- och sjukvården.
Författare:	Moa Malviker Wellermark, Secure State Cyber AB
Handläggare:	Erik Reinicke Projektledare för ”Innovationsmotorer – Ett ekosystem för e-hälsa”
Verksamhet:	Region Östergötland Centrum för verksamhetsstöd och utveckling
Datum och version:	2019-10-30, Version 1.1, Omgjord till extern version

Rapporten är framtagen inom ramen för det nationella projektet Innovationsmotorer. Det drivs av Swedish Medtech inom det strategiska innovationsprogrammet Medtech4Health. Region Östergötlands har ett lokalt projekt som heter ”Innovationsmotorer - Ett ekosystem för E-hälsa”. Projektet är finansierat av Vinnova.

Innehållsförteckning

1 Bakgrund 5

1.1 Begrepp 6

2 Sammanfattning 6

3 Personuppgiftsansvar 6

3.1 Allmänt om personuppgiftsansvar 6

3.2 Personuppgiftsansvar vid egenvård 7

3.2.1 Bedömning av personuppgiftsansvaret i det aktuella fallet 7

3.3 Personuppgiftsansvar vid anlitande av vårdoperatör 8

3.4 Personuppgiftsansvar vid anlitande av extern teknikoperatör 8

4 Dataskyddsförordningen 8

4.1 Principer 8

4.1.1 Laglighet, korrekthet och öppenhet 8

4.1.2 Ändamålsbegränsning 8

4.1.3 Uppgiftsminimering 9

4.1.4 Riktighet 9

4.1.5 Lagringsminimering 9

4.1.6 Integritet och konfidentialitet 9

4.1.7 Ansvarsskyldighet 9

4.2 Inbyggt dataskydd och dataskydd som standard 10

4.3 Anmälan av personuppgiftsbehandling 10

4.4 Konsekvensbedömning enligt dataskyddsförordningen 10

5 Patientdatalagen (2008:355) och Socialstyrelsens föreskrifter och allmänna råd (HSLF-FS 2016:40) 11

5.1 Allmänna utgångspunkter 11

5.2 Vad är en vårdgivare? 11

5.3 Vårdgivare ansvarar för sin egen journal 12

5.4 Möjlighet för flera vårdgivare att dokumentera i samma journalsystem 12

5.5 Innehållet i patientjournal 12

5.6 Inre spärr 13

5.7 Sammanhållen journalföring 13

5.7.1 Grunder 13

5.7.2 Att göra uppgifter tillgängliga för andra vårdgivare 13

5.7.3 Att ta del av uppgifter hos andra vårdgivare 14

5.8 Aktiva val 14

5.8.1 Uppgifter tillhöriga andra vårdenheter/vårdprocesser 14

5.8.2 Uppgifter hos andra vårdgivare 14

5.9 Behandling av personuppgifter i öppna nät 14

5.9.1 Öppna nät 14
5.9.2 Stark autentisering 15
5.10 Styrning av behörigheter 15
5.11 Kontroll av åtkomst till uppgifter 15
5.12 Signering 16
5.13 Förstörande av patientjournal 16
5.14 Bevarande 16
6 Informationsklassning och riskanalys 17
7 Användning av molntjänst 17
7.1 Allmänna utgångspunkter 17
7.2 Offentlighets- och sekretesslagen (2009:400) 17
7.2.1 Allmänna överväganden 17
7.2.2 Justitieombudsmannens beslut den 9 september 2014 (dnr. 3032-2011) 18
7.2.3 eSams rättsliga uttalande den 23 oktober 2018 (VER 2018:57) 19
7.2.4 Juridik som stöd för förvaltningens digitalisering SOU 2018:25 19
7.3 Överföring till tredje land 19
8 Förvaringsrekvisitet för allmänna handlingar enligt 2 kap. 4 § tryckfrihetsförordningen 20
9 Patientens privata enhet 20
Bilaga 1 21

1 Bakgrund

Region Östergötland driver ett projekt, Ekosystem för e-hälsa, som syftar till att underlätta för patienterna att vara delaktiga i sin egen vård, öka tryggheten samt minska behovet av inläggning på sjukhus. Syftet med projektet är även att identifiera, implementera och sprida goda idéer kring hur e-hälsa kan användas för nya och innovativa arbetsprocesser för gruppen multisjuka äldre.

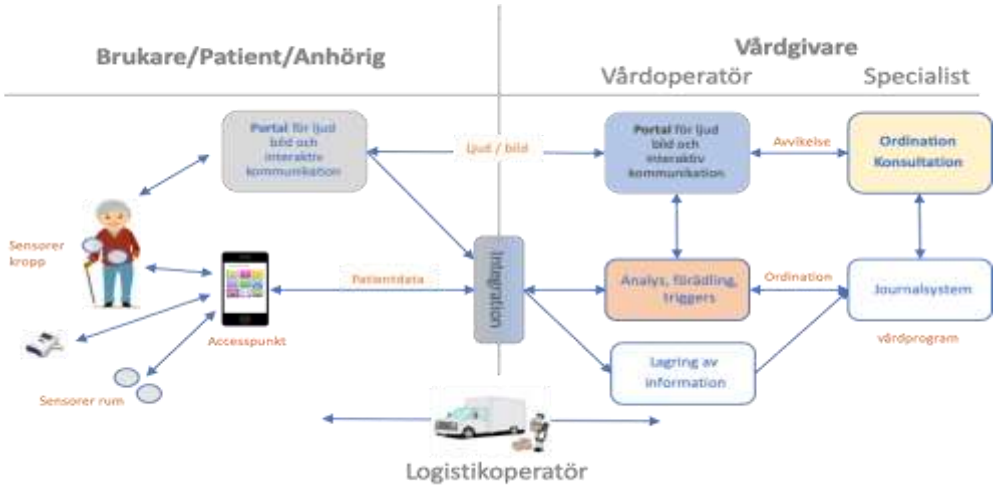
Region Östergötland har inom ramen för projektet anlitat Secure State Cyber AB för att genomföra en genomlysning av informationssäkerhetskraven och de juridiska förutsättningarna för hemmonitorering vid vård. Utgångspunkten för genomlysningen är ett fiktivt exempel som finns beskrivet i rapporten ”Våga vara hemma- Ett ekosystem för E-hälsa”. Genomlysningen ska dock vara generellt applicerbar vid hemmonitorering i hälso- och sjukvården. Det övergripande syftet med genomlysningen är att identifiera vilka juridiska hinder som kan finnas mot hemmonitorering i hälso-och sjukvården och vilka åtgärder som kan vidtas för att överbrygga hindren.

Följande omständigheter föreligger i det fiktiva fallet. Region Östergötland använder sig av en vårdoperatör som hanterar hela patientens sjukdomspanorama och står för den kontinuerliga kontakten med patienten. Vårdoperatören tar emot och analyserar patientens data genererad av e-hälsolösningen i hemmet. Så länge som patienten mår bra hanteras den löpande vården på distans. Vid förändringar i sjukdomsbilden kontaktas berörd specialist för konsultation, vilket typiskt kan leda till remiss för medicinsk diagnostik och/eller justering av vårdprogrammet. Det kan även handla om besök på mottagning. Vårdoperatören verkar mellan patient och specialist. Vårdoperatören kan enklast liknas vid en virtuell vårdcentral som hanterar den löpande dialogen (via telefon, video eller annan digital kanal) med patienten. Vårdoperatören bemannas med sjuksköterskekompetens och vid behov kan frågor eskaleras till läkare, exempelvis vid förändring i sjukdomsbilden. Vårdoperatören signalerar också till teknikoperatören vem som ska ha vilken e-hälsolösning. Funktionen vårdoperatör finns i den egna organisationen men kan i framtiden läggas ut på en privat vårdgivare.

I det fiktiva fallet finns en teknikoperatör som är en extern leverantör som levererar och driftar en e-hälsolösning hos patienten samt en teknikleverantör som är en extern leverantör som levererar och driftar materialhanteringen av e-hälsolösningen hemma hos patienten, vilket inkluderar förbrukningsmaterial, läkemedel och andra produkter som behöver transporteras hem till patienten. Teknikoperatören och teknikleverantören kan i framtiden komma att finnas internt i organisationen.

Ytterligare utgångspunkter för utredningen som har framkommit vid möten med Region Östergötland är att både patienten och vårdgivaren ska kunna komma åt uppgifter som genereras i e-hälsolösningen, att patienten inte ska kunna lagra egna uppgifter utan endast sådana som vårdgivaren bestämmer, att teknikoperatören ska använda en molntjänst som en del i e-hälsolösningen samt att patienten ska kunna använda sin privata mobil/surfplatta.

Nedan finns ett exempel på hur ett informationsflöde i en e-hälsolösning skulle kunna se ut (Illstr. Henrik Schildt).



1.1 Begrepp

Vårdgivare
Den som bedriver hälso- och sjukvård och/eller tandvård t.ex. en region, en kommun eller ett företag

Vårdoperatör
Den vårdgivare som i e-hälsolösningen är mottagare av informationen ifrån patienten. Det kan finnas flera vårdoperatörer.

Logistikoperatör/Teknikleverantör
Den organisation som tillhandahåller apparatur och liknande för att patienten ska kunna översända informationen till vårdoperatören.

Teknikoperatör
Den organisation som levererar och driftar e-hälsolösningen.

E-hälsolösningen
Övergripande begrepp för att beskriva den tekniska lösningen för att uppnå funktionen med hemmonitorering.

2 Sammanfattning

I förevarande rapport har det genomförts en genomlysning av informationssäkerhetskrav och de juridiska förutsättningarna för hemmonitorering i hälso- och sjukvården. Det har inte identifierats några direkta juridiska hinder mot hemmonitorering i hälso- och sjukvården. Genomlysningen har dock resulterat i ett antal bedömningar och förslag på aktiviteter som en region bör vidta för att säkerställa följsamheten mot tillämplig lagstiftning. Bedömningarna och de föreslagna aktiviteterna finns direkt under respektive rubrik löpande i rapporten men de är också samlade i bilaga 1 för att ge en bättre överskådlighet. I bilaga 2 finns förslag på krav, som kan ställas i upphandlingen av e-hälsolösningen, utifrån de bedömningar som gjorts i rapporten.

Bland åtgärdsförslagen finns bland annat att en region bör genomföra en riskanalys och informationsklassificering, teckna personuppgiftsbiträdesavtal, kravställa att en leverantör som behandlar personuppgifter i tredje land på uppdrag av regionen t.ex. använder sig av standardavtalsklausuler eller är anslutna till Privacy Shield, ta fram krav på skyddsåtgärder samt genomföra en konsekvensbedömning.

Genomlysningen innehåller, förutom konkreta åtgärdsförslag, även en allmän redogörelse för tillämplig lagstiftning på området samt de allmänna principer enligt dataskyddsförordningen som en region har att iaktta vid behandling av personuppgifter.

3 Personuppgiftsansvar

3.1 Allmänt om personuppgiftsansvar

Den som är personuppgiftsansvarig är ansvarig för att personuppgiftsbehandlingen är lagenlig. Enligt dataskyddsförordningen är personuppgiftsansvarig den som ensam eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter.[1] Datainspektionen har i olika sammanhang uttalat att det är de faktiska förhållandena i det enskilda fallet som är avgörande, dvs. vem eller vilka som faktiskt bestämmer över personuppgiftsbehandlingen.

Vem som är personuppgiftsansvarig kan även anges i lag eller förordning. Så är fallet när en vårdgivare behandlar personuppgifter. Enligt patientdatalagen är en vårdgivare personuppgiftsansvarig för den behandling av personuppgifter som vårdgivaren utför[2].

[1] Dataskyddsförordningen 2016/679 artikel 4
[2] Patientdatalagen 2008:355 2 kap 6§

Med personuppgiftsbiträde avses den som behandlar personuppgifter för den personuppgiftsansvariges räkning. Personuppgiftsbiträdet ska behandla personuppgifter i enlighet med den personuppgiftsansvariges instruktioner.[3]

3.2 Personuppgiftsansvar vid egenvård

Bestämmelser om egenvård finns i Socialstyrelsens föreskrifter (SOSFS 2009:6) om bedömningen av om en hälso- och sjukvårdsåtgärd kan utföras som egenvård. Med egenvård avses enligt föreskrifterna en hälso- och sjukvårdsåtgärd som legitimerad hälso- och sjukvårdspersonal bedömt att en patient själv kan utföra. Däremot är hälso- och sjukvårdens bedömning, planering och uppföljning att betrakta som hälso- och sjukvård.

Det går inte att säga generellt vilka åtgärder som utgör egenvård utan det beror på omständigheterna i varje enskilt fall. Av föreskrifterna framgår att yrkesutövarens bedömning ska göras i samråd med patienten och utifrån respekten för dennes självbestämmande och integritet samt behov av trygghet och säkerhet. Bedömningen ska utgå från patientens fysiska och psykiska hälsa samt dennes livssituation. Som en del i bedömningen ska det ingå en analys av om utförandet av egenvården kan innebära att patienten utsätts för risk att skadas (riskanalys). I förekommande fall ska en utredning göras för att avgöra om patienten själv eller med hjälp av någon annan på ett säkert sätt kan utföra en hälso- och sjukvårdsåtgärd som egenvård. Av landstingens rutiner för egenvård framgår genomgående att behandling som kräver omfattande instruktioner och handledd träning av ansvarig läkare eller annan legitimerad hälso- och sjukvårdspersonal är hälso- och sjukvård, inte egenvård.

Enligt Socialstyrelsens föreskrifter utgör egenvård i föreskrifternas mening inte hälso- och sjukvård. Det innebär att om patientens egenmätningar i hemmet utgör egenvård så förutsätts att personuppgiftsbehandlingen i mätutrustningen och i det personliga hälsokontot är av ren privat natur. I dessa fall är det patienten som rent faktiskt råder över personuppgiftsbehandlingen, inte vårdgivaren.

Det är omständigheterna i det enskilda fallet som avgör om en vårdgivare blir personuppgiftsansvarig samt i vilken utsträckning eller om det handlar om patientens egen behandling av personuppgifter som är av rent privat natur. Detta är en fråga som slutligen bestäms av varje vårdgivare själv. Faktorer som kan påverka denna bedömning är t.ex. i vilken utsträckning vårdgivaren bestämmer över personuppgiftsbehandlingen genom att exempelvis instruera vilka data som ska lämnas ut och i vilka intervaller eller om patientens aktiviteter snarare utgör hälso- och sjukvård än egenvård. Ytterligare omständigheter som talar för att vårdgivaren har ett utsträckt personuppgiftsansvar för patientens personuppgiftsbehandling är att vårdgivaren tillhandahåller eller finansierar mätutrustningen eller det personliga kontot.

3.2.1 Bedömning av personuppgiftsansvaret i det aktuella fallet

Målet med projektet ”Ett ekosystem för e-hälsa” är att möjliggöra vård på distans. Upplägget kan enklast liknas vid en virtuell vårdcentral som hanterar den löpande dialogen (via telefon, video eller annan digital kanal) med patienten för aktuell diagnos. Projektet är inte avgränsat till de fall där man har bedömt att patienten kan utföra sin vård själv eller med hjälp av någon. Tanken är att det ska finnas en vårdoperatör bestående av sjuksköterskekompetens som sköter den löpande kontakten med patienten och vid behov eskalerar till specialist. Regionen tillhandahåller all utrustning. Dock ska patienten kunna använda sin privata mobil/surfplatta. En förutsättning är också att patienten inte ska kunna lagra egna uppgifter utan endast sådana som vårdgivaren bestämmer. I det stora hela bör därför utgångspunkten vara att regionen är personuppgiftsansvarig för den behandling av personuppgifter som sker vid vård på distans.

Resonemanget hindrar inte i sig att E-hälsolösningen även kan användas i fall av egenvård men när det blir aktuellt bör regionen dokumentera tydligt vilka delar med tillhörande personuppgifter som regionen anser är egenvård och att patienten är ansvarig för denna behandling så att detta särskiljs.

[3] Dataskyddsförordningen 2016/679 artikel 4

3.3 Personuppgiftsansvar vid anlitande av vårdoperatör

Utgångspunkten i det fiktiva fallet är att all vård av patient ska ske internt inom regionen, men vården kan dock komma att läggas ut på extern part i framtiden t.ex. en privat vårdgivare. Det kan också bli aktuellt att delar av vården i samband med monitoreringen genomförs av en annan region eller av en kommun. Av patientdatalagen framgår att varje vårdgivare är ansvarig för sin personuppgiftsbehandling[4]. För det fall att vården eller delar av vården genomförs av en annan vårdgivare än regionen ansvarar denne således för sin personuppgiftsbehandling.

Det är vidare viktigt att patientdalalagens regler gällande exempelvis sammanhållen journalföring följs om regionen och den externa vårdgivaren ska ta del av varandras information.

3.4 Personuppgiftsansvar vid anlitande av extern teknikoperatör

I det fiktiva fallet finns en teknikoperatör som är en extern leverantör som levererar och driftar en e-hälsolösning. Teknikoperatören kommer som en del i sin leverans att behandla personuppgifter för regionens räkning. Regionen måste därför teckna ett personuppgiftsbiträdesavtal med leverantören som reglerar hur leverantören ska hantera personuppgifterna för regionens räkning.

Bedömning/aktivitet
Teckna personuppgiftsbiträdesavtal vid anlitande av extern teknikoperatör som behandlar personuppgifter på uppdrag av en region alternativt har potentiell åtkomst till regionens personuppgifter.

4 Dataskyddsförordningen

4.1 Principer

Dataskyddsförordningen med kompletterande lagstiftning, så som t.ex. dataskyddslagen, är en förordning som är direkt tillämplig i Sverige. Förordningen innehåller vissa allmänna principer som verksamheten har att utgå ifrån i arbetet med projektet Ett ekosystem för e-hälsa. Nedan följer en redogörelse för dessa principer.

4.1.1 Laglighet, korrekthet och öppenhet

All personuppgiftsbehandling måste vara laglig, korrekt och präglas av öppenhet. Att personuppgiftsbehandlingen ska vara laglig innebär att det måste finnas en rättslig grund för personuppgiftsbehandlingen och att övriga principer och bestämmelser i dataskyddsförordningen och i annan kompletterande lagstiftning ska följas. Behandlingen av personuppgifter ska vara rättvis, skälig, rimlig och proportionerlig i förhållande till de registrerade. Det ska också vara klart och tydligt för de registrerade hur deras personuppgifter behandlas.[5]

4.1.2 Ändamålsbegränsning

En viktig princip i dataskyddsförordningen är att personuppgifter endast får samlas in för särskilda, uttryckligt angivna och berättigade ändamål. Ändamålen måste vara specifika och konkreta, inte luddiga eller otydliga. Ändamålet ska vidare vara berättigat, dvs. att personuppgiftsbehandlingen ska ha en rättslig

[4] Patientdatalagen 2008:355 2 kap 6§
[5] Dataskyddsförordningen 2016/679 artikel 5

grund och att den ska ske i enlighet med övrig tillämplig lagstiftning och allmänna rättsprinciper. Ändamålet sätter också ramarna för vad som får och inte får behandlas. Om de insamlade personuppgifterna ska behandlas på ett helt nytt sätt, måste det ske på ett sätt som är förenligt med de ursprungliga ändamålen.[6]

4.1.3 Uppgiftsminimering

Endast de personuppgifter som är nödvändiga för att uppnå syftet med behandlingen får hanteras.[7]

4.1.4 Riktighet

Personuppgifterna ska vara riktiga och, i tillämpliga fall, uppdaterade. Om uppgifterna inte är korrekta ska de rättas eller raderas.[8]

4.1.5 Lagringsminimering

Personuppgifter får endast sparas så länge det är nödvändigt för att uppnå ändamålet med personuppgiftsbehandlingen[9]. När personuppgifterna inte längre behövs ska de raderas eller avidentifieras. Det är därför viktigt att det finns rutiner för gallring. Här är det dock viktigt att tänka på annan lagstiftning kan kräva att uppgifterna ändå bevaras såsom t.ex. arkivlagen.

4.1.6 Integritet och konfidentialitet

Alla personuppgifter ska skyddas så att ingen obehörig kommer åt dem och så att de inte används på ett otillåtet sätt. Lämpliga tekniska och organisatoriska åtgärder ska därför vidtas för att skydda personuppgifterna.[10] En utgångspunkt är de krav som informationsklassning, riskanalys och eventuell konsekvensanalys utmynnar i. Exempel på skyddsåtgärder är behörighetsstyrning, autentisering/identifiering och skydd vid överföring och kommunikation (kryptering). I patientdatalagen, som är en speciallagstiftning som kompletterar dataskyddsförordningen, anges uttryckligen vilka säkerhetsåtgärder som ska vidtas i tillämpliga fall[11].

Bedömning/Aktivitet
Regionen bör ta fram krav på skyddsåtgärder utifrån denna rapport och genomföra en riskanalys och informationsklassificering för att även få fram krav därifrån. Detta för att säkerställa att dessa krav definieras och ställs så att adekvata skyddsåtgärder kommer med i upphandlingen av hemmonitoreringslösningen.

4.1.7 Ansvarsskyldighet

I och med dataskyddsförordningen finns utöver en skyldighet att följa grundläggande principer även en skyldighet att kunna visa att principerna följs samt på vilket sätt. Några sätt att visa på att de grundläggande principerna följs är att lämna tydlig information till de registrerade, föra register över och dokumentera de personuppgiftsbehandlingar som pågår i organisationen, upprätta interna riktlinjer, bygga in

[6] Dataskyddsförordningen 2016/679 artikel 5
[7] Dataskyddsförordningen 2016/679 artikel 5
[8] Dataskyddsförordningen 2016/679 artikel 5
[9] Dataskyddsförordningen 2016/679 artikel 5
[10] Dataskyddsförordningen 2016/679 artikel 5
[11] Patientdatalagen 2008:355 kap 4 och 6

integritetsvänliga lösningar i systemen (så kallat inbyggt dataskydd) samt att göra konsekvensbedömningar innan personuppgiftsbehandlingar som innebär särskilda integritetsrisker påbörjas.[12]

4.2 Inbyggt dataskydd och dataskydd som standard

Inbyggt dataskydd (privacy by design) innebär att man redan vid utformningen av IT-system och rutiner har integritetsskyddsreglerna i åtanke. Kravet på dataskydd som standard (privacy by default) innebär att den som behandlar personuppgifter ska se till att personuppgifter i standardfallet inte behandlas i onödan, exempelvis genom förvalda inställningar så att inte fler personuppgifter än nödvändigt hanteras.[13]

4.3 Anmälan av personuppgiftsbehandling

En region är skyldig att som personuppgiftsansvarig föra register över sina personuppgiftsbehandlingar[14]. Personuppgiftsbehandlingen, alltså själva behandlingen av personuppgifterna i samband med hemmonitoreringen, ska därför anmälas till regionens register över personuppgiftsbehandlingar om detta inte finns anmält sedan tidigare.

Bedömning/Aktivitet
Behandlingen av personuppgifter som sker via hemmonitoreringen behöver anmälas till regionens förteckning av personuppgiftsbehandlingar.

4.4 Konsekvensbedömning enligt dataskyddsförordningen

All personuppgiftsbehandling medför någon form av risk för att den enskildes personliga integritet kränks. Genom dataskyddsförordningen införs ett nytt krav på att genomföra konsekvensbedömningar innan vissa personuppgiftsbehandlingar påbörjas som sannolikt medför en *hög risk* för individens integritet. Det innebär att den risk som behandlingen medför för individens integritet ska utvärderas och möjliga skyddsåtgärder identifieras.[15]

Det finns huvudsakligen tre mål med en sådan analys:

- Att säkra efterlevnaden av dataskyddslagstiftningen.
- Att identifiera riskerna och konsekvenserna för den personliga integriteten.
- Att utifrån riskerna identifiera åtgärder och alternativa tillvägagångssätt för att eliminera, minska eller i vissa fall acceptera de potentiella integritetsriskerna förutsatt att lämpliga säkerhetsåtgärder är vidtagna.

I konsekvensbedömningen ska bl.a. den planerade behandlingen beskrivas utförligt och de potentiella riskerna för den personliga integriteten ska identifieras. När riskerna är identifierade ska lämpliga skyddsåtgärder föreslås för att eliminera eller minska de identifierade riskerna.

Om det, trots att skyddsåtgärder har identifierats genom konsekvensbedömningen, kvarstår hög risk för den personliga integriteten, *måste* samråd ske med Datainspektionen innan personuppgiftsbehandlingen genomförs. Detta för att Datainspektionen ska kunna ge förslag på hur den enskilda integriteten bättre kan skyddas.

En region behöver göra en bedömning av om konsekvensbedömning enligt dataskyddsförordningen ska genomföras. Om bedömningen är att en sådan ska genomföras bör detta ske på ett så tidigt stadium som

[12] Dataskyddsförordningen 2016/679 artikel 5
[13] Dataskyddsförordningen 2016/679 artikel 25
[14] Dataskyddsförordningen 2016/679 artikel 30
[15] Dataskyddsförordningen 2016/679 artikel 35

möjligt. Om bedömningen utmynnar i att konsekvensbedömning inte ska genomföras så ska detta dokumenteras. Regionen har riktlinjer för hur konsekvensbedömningar ska genomföras.

Om en region har som avsikt att behandla en stor mängd känsliga uppgifter i e-hälsolösningar som inte använts i så stor utsträckning tidigare med eventuellt nya tekniska lösningar, är det lämpligt att regionen genomför en konsekvensbedömning.

Bedömning/Aktivitet
En region bör genomföra en konsekvensbedömning.

5 Patientdatalagen (2008:355) och Socialstyrelsens föreskrifter och allmänna råd (HSLF-FS 2016:40)

5.1 Allmänna utgångspunkter

Patientdatalagen är en särskild registerlag som specifikt reglerar hur personuppgifter ska hanteras inom hälso- och sjukvården. Syftet är att skydda patientens integritet och öka patientsäkerheten. Lagen reglerar bland annat möjligheten för olika vårdgivare att ta del av varandras personuppgifter genom sammanhållen journalföring.

Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården; HSLF-FS 2016:40, kompletterar bestämmelserna i patientdatalagen.

Med hälso- och sjukvård avses bland annat verksamhet enligt hälso- och sjukvårdslagen[16]. I patientdatalagen anges uttryckligen för vilka ändamål personuppgifter får behandlas inom hälso- och sjukvården och därmed lagens tillämpningsområde[17]. Av de angivna ändamålen kan slutsatsen dras att patientdatalagens krav inte enbart omfattar den personuppgiftshantering som sker vid förande av patientjournal.

Bedömning/Aktivitet
Patientdatalagen blir tillämplig på hemmonitoreringslösningen så länge vården är att se som hälso- och sjukvård.

5.2 Vad är en vårdgivare?

En vårdgivare är en statlig myndighet, landsting eller kommun (offentlig vårdgivare) samt annan juridisk person eller enskild näringsidkare som bedriver hälso- och sjukvårdsverksamhet (privat vårdgivare).[18] En privat aktör är en enskild privat vårdgivare oavsett om aktören är upphandlad eller på annat sätt anlitad att på en huvudmans ansvar tillhandahålla vård inom ett visst geografiskt område. I exempelvis Östergötland är regionen att betrakta som en vårdgivare medan varje övrig enskild organisation som tillhandahåller vård inom Östergötland är att betrakta som en annan vårdgivare, d.v.s. även avtalade vårdgivare är i den bemärkelsen helt fristående från regionen.

[16] Patientdatalagen 2008:355 1 kap 3§
[17] Patientdatalagen 2008:355 2 kap 4§
[18] Patientdatalagen 2008:355 1 kap 3§

Bedömning/Aktivitet
En region bör säkerställa att det tydligt framgår i aktuell upphandling och efterkommande avtal om avsikten är att upphandla en vårdgivare (vårdoperatör) dvs. en privat vårdgivare som ansvarar för sin egen personuppgiftsbehandling eller om avsikten istället är att upphandla en teknikoperatör eller teknikleverantör. Detta har betydelse vem som är ansvarig för personuppgiftsbehandlingen samt vem som bär det medicinska ansvaret för vården som bedrivs.

5.3 Vårdgivare ansvarar för sin egen journal

Vid vård av patienter ska det föras patientjournal[19]. Varje vårdgivare är personuppgiftsansvarig för den behandling av personuppgifter som sker inom den egna verksamheten[20]. Det innebär bland annat att varje vårdgivare är ansvarig för sin journalföring. Det råder också som huvudregel sekretess mellan vårdgivarna, vilket innebär att något undantag ifrån sekretessen måste vara uppfyllt för att uppgifter ska kunna föras över mellan flera vårdgivare.[21]

5.4 Möjlighet för flera vårdgivare att dokumentera i samma journalsystem

Kravet att varje vårdgivare för sin egen journal, innebär inte att det finns hinder mot att flera vårdgivare använder samma system för journalföring. Det förutsätter dock att vårdgivarnas uppgifter är separerade från varandra samt att vårdgivarna i övrigt kan uppfylla sina skyldigheter enligt patientdatalagen, offentlighets- och sekretesslagen samt annan tillämplig lagstiftning.

5.5 Innehållet i patientjournal

En patientjournal får innehålla uppgifter som behövs för att fullgöra skyldigheten att föra patientjournal och upprätta annan dokumentation som behövs för vården av patienten, eller administration som rör patienten och som syftar till att ge vård i enskilda fall eller som annars motiveras av vård i enskilda fall.[22]

Enligt de grundläggande bestämmelserna i patientdatalagen ska patientjournalen innehålla de uppgifter som behövs för en god och säker vård av patienten. Under förutsättning att uppgifterna finns tillgängliga ska patientjournalen alltid innehålla

- uppgifter om patientens identitet,
- väsentliga uppgifter om bakgrunden till vården,
- uppgifter om diagnos och anledning till mer framstående åtgärder,
- väsentliga uppgifter om genomförda och planerade åtgärder,
- uppgifter om informationen som lämnats till patienten, hens vårdnadshavare och övriga närstående,
- uppgifter om ställningstaganden som gjorts om val av behandlingsalternativ och möjligheten till ny medicinsk bedömning,
- uppgifter om att patienten valt att avstå från vård eller behandling och
- uppgifter om vem som har gjort en viss anteckning och när anteckningen gjordes.[23]

I andra författningar finns kompletterande regler om patientjournalens innehåll, till exempel i 5 kap. 5 § Socialstyrelsens föreskrifter HSLF-FS 2016:40.

[19] Patientdatalagen 2008:355 3 kap 1§
[20] Patientdatalagen 2008:355 2 kap 6§
[21] Offentlighets- och sekretesslagen 2009:400 25 kap 1§
[22] Patientdatalagen 2008:355 3 kap 5§
[23] Patientdatalagen 2008:355 3 kap 6§

Uppgifter som ska antecknas i patientjournal ska föras in så snart som möjligt[24].

Bedömning/Aktivitet
En region kommer att behöva ta ställning till vilka delar av uppgifterna, som överförs ifrån patienten via hemmonitoreringslösningen till vården, som ska vara och är en del av patientens journal. Dessa uppgifter styrs av särskilda regler gällande t.ex. bevarande och möjlighet att delge andra vårdgivare via system för sammanhållen journalföring. Regionen kommer antagligen också behöva ta ställning till om de uppgifter som utgör journal ska överföras till ett visst journalsystem/lagringsyta inom regionen. Detta är dock inte avgörande för att lösningen ska kunna tas i bruk även om den bör lösas ut i närtid.

5.6 Inre spärr

Patienten har rätt att motsätta sig att uppgifter görs elektroniskt tillgängliga för andra vårdenheter eller vårdprocesser än den som ansvarar för uppgifterna (inre spärr). Uppgifterna ska i sådana fall spärras för andra vårdenheter och vårdprocesser.[25] Patienten kan begära spärr närsomhelst. Spärren avser endast åtkomst i vårdsyfte. Uppgifterna får således vara tillgängliga för andra syften, t.ex. administration och uppföljning. En spärr får hävas om patienten samtycker till det samt i akutsituationer då patienten inte kan lämna sitt samtycke pga. exempelvis medvetslöshet.[26] För att vårdgivaren ska kunna fullgöra sin skyldighet att spärra uppgifter krävs att vårdgivaren har fastställt vårdenheter och vårdprocesser i den egna verksamheten. I en vårdprocess kan flera vårdenheter ingå och i sådana fall gäller spärren mot utomstående vårdenheter som inte ingår i den vårdprocessen.

Bedömning/Aktivitet
Om en region beslutar att patientuppgifterna i hemmonitoreringslösningen ska vara åtkomlig för fler vårdenheter, så att de kan se varandras patientuppgifter, behöver regionen ställa krav på funktion av inre spärr.

5.7 Sammanhållen journalföring

5.7.1 Grunder

Genom sammanhållen journalföring ges en möjlighet för vårdgivare att ta del av varandras patientuppgifter genom direktåtkomst. Till skillnad mot traditionellt informationsutbyte genom utlämnande av information efter begäran, ger reglerna om sammanhållen journalföring vårdgivarna möjlighet att få elektronisk tillgång till varandras patientuppgifter direkt. Reglerna om sammanhållen journalföring är indelade i två steg[27]. Det första steget reglerar under vilka förutsättningar vårdgivare får göra patientuppgifterna tillgängliga för andra vårdgivare. Det andra steget reglerar under vilka förutsättningar vårdgivare får ta del av patientuppgifter som andra vårdgivare har tillgängliggjort.

5.7.2 Att göra uppgifter tillgängliga för andra vårdgivare

Endast uppgifter som är dokumenterade i vårdsyfte får göras tillgängliga mellan vårdgivare genom sammanhållen journalföring. [28] Innan uppgifterna görs tillgängliga ska patienten informeras om vad det innebär och att patienten har möjlighet att motsätta sig att delta i sammanhållen journalföring. Om patienten inte har motsatt sig får uppgifterna göras tillgängliga i system för sammanhållen journalföring.[29]

[24] Patientdatalagen 2008:355 3 kap 9§
[25] Patientdatalagen 2008:355 4 kap 4§
[26] Patientdatalagen 2008:355 4 kap 5§
[27] Patientdatalagen 2008:355 6 kap 2§
[28] Patientdatalagen 2008:355 6 kap 1§
[29] Patientdatalagen 2008:355 6 kap 2§

5.7.3 Att ta del av uppgifter hos andra vårdgivare

En vårdgivare får ta del av andra vårdgivares patientuppgifter om uppgifterna kan antas ha betydelse för att förebygga, utreda eller behandla sjukdomar och skador hos patienten eller för att utfärda intyg om vården. Vårdgivaren måste dessutom ha en aktuell patientrelation med patienten och patientens samtycke till att ta del av uppgifterna.[30]

Bedömning/Aktivitet
Om en region beslutar att patientuppgifterna i hemmonitoreringslösningen ska vara åtkomlig för flera vårdgivare via system för sammanhållen journalföring, så att de kan se varandras patientuppgifter, behöver regionen ställa krav på funktion för yttre spärr, samtyckeshantering och nödöppning.

5.8 Aktiva val

5.8.1 Uppgifter tillhöriga andra vårdenheter/vårdprocesser

Information om på vilka andra vårdenheter eller i vilka andra vårdprocesser det finns uppgifter om en patient, får inte göras tillgänglig utan att användare tar ställning till om denne är behörig att ta del av uppgifterna (aktivt val). Uppgifterna om patienten får sedan inte göras tillgängliga utan att användaren gör ytterligare ett aktivt val. För det fall det finns förutsättningar att ta del av spärrade uppgifter får uppgifterna inte göras tillgängliga utan att det föregås av ett aktivt val.[31]

Bedömning/Aktivitet
Om en region beslutar att patientuppgifterna i hemmonitoreringslösningen ska vara åtkomlig för fler vårdenheter, så att de kan se varandras patientuppgifter, behöver regionen ställa krav på funktion av aktiva val.

5.8.2 Uppgifter hos andra vårdgivare

Åtkomst till ospärrade uppgifter om en patient vid sammanhållen journalföring får endast ske efter föregående aktivt val från användaren.[32]

Bedömning/Aktivitet
Om en region beslutar att patientuppgifterna i hemmonitoreringslösningen ska vara åtkomlig för flera vårdgivare via system för sammanhållen journalföring, så att de kan se varandras patientuppgifter, behöver regionen ställa krav på funktion för aktiva val.

5.9 Behandling av personuppgifter i öppna nät

5.9.1 Öppna nät

Om en vårdgivare använder öppna nät vid behandling av personuppgifter, ska denne ansvara för att överföringen av uppgifterna görs på ett sådant sätt att inte obehöriga kan ta del av dem, och elektronisk åtkomst eller direktåtkomst till uppgifterna föregås av stark autentisering.[33]

[30] Patientdatalagen 2008:355 6 kap 3-3a§§
[31] HSLF-FS 2016:40 4 kap 4§
[32] HSLF-FS 2016:40 4 kap 6§
[33] HSLF-FS 2016:40 3 kap 15§

Öppna nät kan beskrivas som datornätverk som en enskild användare har tillgång till, exempelvis internet. Genom att utnyttja internet är det möjligt att kommunicera enkelt och effektivt. Om inte vårdgivaren vidtar särskilda skyddsåtgärder kommer dock informationen att överföras oskyddad. Därför är det nödvändigt med specifika säkerhetslösningar för att minska risken för att obehöriga personer tillgång till informationen.

Då e-hälsolösningen med största sannolikhet kommer innebär en överföring av patientuppgifter över öppna nät behöver lösningen se till så att ingen obehörig kan nå uppgifterna. I praktiken innebär det bland annat att uppgifter om patienter måste skyddas genom att de överförs genom en krypterad förbindelse eller genom att kryptera själva uppgifterna.

Bedömning/Aktiviteter
Regionen behöver säkerställa att e-hälsolösningen har insynsskydd så att ingen obehörig kommer åt uppgifterna.

5.9.2 Stark autentisering

För att en behörig användare ska få tillgång till personuppgifter via öppna nät måste vårdgivaren se till att åtkomsten föregås av en så kallad stark autentisering[34]. Det innebär att vårdgivaren använder inloggningslösningar som ställer krav på att identiteten kontrolleras på minst två olika sätt. En etablerad metod för stark autentisering är att använda en e-legitimation men det finns många tekniska lösningar för att uppnå en stark autentisering. Lagstiftaren har inte angett vilken metod som måste användas utan detta är upp till en region att använda.

Bedömning/Aktivitet
En region bör kravställa funktion för stark autentisering för åtkomst till patientuppgifterna via e-hälsolösningen, både för hälso- och sjukvårdspersonal och patienter.

5.10 Styrning av behörigheter

Vårdgivaren ska bestämma villkoren för tilldelning av behörighet för åtkomst till uppgifter om patienter. Behörigheten ska begränsas till vad som behövs för att den enskilde ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården.[35] Vårdgivaren ansvarar vidare för att varje användare tilldelas en individuell behörighet[36]. Det innebär bland annat att endast personliga inloggningar är tillåtna och att inga så kallade gruppkonton får förekomma.

Bedömning/Aktivitet
En region bör ha styrande dokument och rutiner för styrning av behörigheter vilka behöver följas.

5.11 Kontroll av åtkomst till uppgifter

Vårdgivaren ska se till att åtkomst till uppgifter om patienter dokumenteras och kan kontrolleras. Av dokumentationen av åtkomsten (loggar) ska det framgå

- vilka åtgärder som har vidtagits med uppgifter om en patient t.ex. registrerat analyssvar och läst analyssvar,
- vid vilken vårdenhet eller vårdprocess åtgärderna vidtagits,
- vid vilken tidpunkt åtgärderna vidtagits, och

[34] HSLF-FS 2016:40 3 kap 15§
[35] Patientdatalagen 2008:355 4 kap 2§
[36] HSLF-FS 2016:40 4 kap 2§

- användarens och patientens identitet.[37]

Bedömning/Aktivitet
En region behöver kravställa på en loggfunktion som innehåller de parametrar som Socialstyrelsens föreskrifter anger (åtgärd, vårdenhet/vårdprocess, tidpunkt och identiteterna på användaren och patienten). Om en region har för avsikt att överföra dessa loggar till en gemensam logglösning behöver även dessa krav omhändertas.

5.12 Signering

Vårdgivaren ska säkerställa att det finns rutiner för signering av journalhandlingar avseende en patients vård och behandling[38]. I och med att det idag är oklart hur uppgifterna som kommer ifrån patienten ska överföras ifrån e-hälsolösningen till regionens egna IT-stöd, om det ska ske överhuvudtaget, är det svårt att uttala sig om kravet på signering och var denna bekräftelse bör ligga. Utifrån uppgifternas karaktär är det dock lämpligt att det sker någon form av bekräftelse när hälso- och sjukvårdspersonalen tar del av uppgifterna ifrån patienten för att visa att uppgifterna är lästa och att någon tagit ansvar för att vidta eventuella åtgärder alternativt fattat beslut om att det inte behöver vidtas några åtgärder.

Bedömning/Aktivitet
En region bör kravställa på en funktion för bekräftelse/signering.

5.13 Förstörande av patientjournal

Vårdgivaren ska säkerställa att uppgifter i en patientjournal inte kan förstöras annat än med stöd av patientdatalagen. På ansökan av en patienten eller någon annan som omnämns i en patientjournal får Inspektionen för vård och omsorg besluta att journalen helt eller delvis ska förstöras.[39] Det ska därför vara möjligt att förstöra/radera patientuppgifter på administratörsnivå. Beroende på om regionen bedömer att uppgifterna i e-Hälsolösningen är att anse som patientjournal eller inte kan det finnas behov av en funktion för förstörande av patientjournal.

Bedömning/Aktivitet
Om en region bedömer att uppgifterna i e-hälsolösningen är patientjournal bör regionen säkerställa att det går att förstöra (radera) uppgifterna i e-hälsolösningen.

5.14 Bevarande

Enligt patientdatalagen ska en journalhandling sparas i minst tio år efter det att den sista uppgiften fördes in i handlingen[40]. Loggarna ska sparas minst fem år för att möjliggöra kontroll av åtkomsten till uppgifter om en patient[41]. En region omfattas dock också av arkivlagen vilket gör att bevarandetiderna oftast blir betydligt längre.

Bedömning/Aktivitet
Beroende på lösning av överföring av patientuppgifter ifrån e-hälsolösningen bör Regionarkivet involveras för att kunna ställa specifika krav kopplade till bevarandet av uppgifterna. Detta är dock inte avgörande för att lösningen ska kunna tas i bruk även om det bör lösas ut i närtid.

[37] HSLF-FS 2016:40 4 kap 9§
[38] Patientdatalagen 2008:355 3 kap 10§
[39] Patientdatalagen 2008:355 8 kap 4§
[40] Patientdatalagen 2008:355 3 kap 17§
[41] HSLF-FS 2016:40 4 kap 9§

6 Informationsklassning och riskanalys

Innan anskaffning, nyutveckling eller förändring av organisationens IT-stöd eller infrastruktur, bör en informationsklassificering av informationen genomföras. I samband med informationsklassificeringen är det även bra att genomföra en riskanalys i syfte att identifiera olika risker med informationshanteringen.

Informationsklassificeringen och riskanalysen ska ge verksamheten vägledning kring vilka skyddsåtgärder som behövs och därmed vilka krav som behöver ställas på en eventuell leverantör för att dessa ska uppfyllas. Det är därför viktigt att kravställningen görs innan upphandling eller egenutveckling av system. Informationsklassificeringen och riskanalysen har både till syfte att definiera rätt nivå av säkerhetsskydd men bidrar också till att skapa tillit till e-hälsolösningen.

Bedömning/Aktivitet
En region bör genomföra en riskanalys och informationsklassificering för att skapa tillit och få fram adekvata krav på organisatoriska och tekniska skyddsåtgärder. Detta bör med fördel genomföras innan kraven i aktuell upphandling fastställs.

7 Användning av molntjänst

7.1 Allmänna utgångspunkter

Den som använder en molntjänst för sin personuppgiftsbehandling är personuppgiftsansvarig för behandlingen även om den utförs av en molntjänstleverantör eller dess underleverantörer. Leverantören och dess underleverantörer som anlitas för behandlingen är personuppgiftsbiträden. Den personuppgiftsansvarige ansvarar för att hanteringen av information i en molntjänst följer tillämplig lagstiftning såsom t.ex. dataskyddsförordningen, patientdatalagen och offentlighets- och sekretesslagen.

Ett personuppgiftsbiträdesavtal behöver också tecknas med molntjänstleverantören där den personuppgiftsansvarige bestämmer hur personuppgifterna i molntjänsten ska behandlas samt vilka instruktioner personuppgiftsbiträdet ska följa.

En risk- och sårbarhetsanalys behöver genomföras av den personuppgiftsansvarige för att bedöma om det är möjligt att använda den aktuella molntjänsten för den tänkta personuppgiftsbehandlingen. Nödvändiga säkerhetsåtgärder behöver vidtas vid användningen av molntjänsten.

En region bör har styrande dokument för användning av molntjänster.

Bedömning/Aktivitet
En region bör genomföra en risk- och sårbarhetsanalys. Denna analys bör dock kunna genomföras tillsammans med övriga analyser (riskanalys, konsekvensbedömning och informationsklassificering) så att dubbelarbete undviks och att resultat uppnås så snabbt som möjligt.

7.2 Offentlighets- och sekretesslagen (2009:400)

7.2.1 Allmänna överväganden

Offentlighets- och sekretesslagen påverkar myndigheters möjlighet att använda molntjänster. Enligt 25 kap. 1 § offentlighets- och sekretesslagen gäller sekretess inom hälso- och sjukvården för uppgift om en enskilds hälsotillstånd eller andra personliga förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till denne lider men. Frågan om en vårdgivare kan lämna ut sekretessbelagda

uppgifter till ett personuppgiftsbiträde eller till personal hos biträdet ska prövas på vanligt sätt enligt offentlighets- och sekretesslagen.

En myndighet som överväger användning av en molntjänst måste göra en noggrann analys av om ett utlämnande till molntjänstleverantören kan ske enligt relevanta sekretessbestämmelser. Eftersom det normalt saknas tillämpliga undantagsbestämmelser blir den centrala rättsliga frågan om skada eller men uppstår vid användningen av tjänsten. En sådan bedömning måste utgå från omständigheterna i det enskilda fallet. För det första är det relevant vilken typ av sekretessbelagda uppgifter som kommer att omfattas av utlämnandet. För det andra är tjänstens faktiska och rättsliga utformning relevant. Om uppgifterna skyddas väl hos leverantören är risken för skada och men inte större än hos myndigheten. Centrala frågor i sammanhanget är hur obehörig åtkomst till uppgifterna motverkas samt hur spridning och annan obehörig användning av uppgifter som någon, till exempel en anställd hos leverantören, lagligen fått tillgång till motverkas. I detta sammanhang är inte bara IT-säkerhetssystemens utformning relevanta, utan även instruktioner till och avtal med personal, liksom förekomsten av anknytande straffrättsligt skydd, till exempel i form av regler om dataintrång.

Det är svårt att uttala sig generellt om molntjänster och dess risker eftersom riskerna helt bygger på molntjänstens användning, uppgifterna som ska behandlas, vilken typ av säkerhetsåtgärder som finns tillgängliga samt i vilket land lagring och underleverantören befinner sig. Det går dock att säga att det är en risk i sig att använda molntjänster för känsliga personuppgifter såsom patientuppgifter. Denna risk går att minska genom att vidta adekvata åtgärder såsom tillexempel kryptering, där krypteringsnycklarna inte är tillgängliga för underleverantören. Beroende på i vilket land lagringen sker och var underleverantören har sitt säte går det också att öka eller minska riskerna. Att lagra patientuppgifterna i ett tredje land utanför EU eller via ett företag som har sitt säte utanför EU t.ex. USA bör vara en större risk än ett företag som är etablerat och har sin lagring inom EU eftersom det minskar risken för röjande av uppgifterna.

Bedömning/Aktivitet
En region behöver ta ställning till om aktuella patientuppgifter kan lämnas ut till de aktuella personuppgiftsbiträdena i e-hälsolösningen utifrån regelverket i offentlighets- och sekretesslagen. Det innebär att regionen behöver ta ställning till om det finns sekretesshinder.

7.2.2 Justitieombudsmannens beslut den 9 september 2014 (dnr. 3032-2011)

Av betydelse i sammanhanget är att Justitieombudsmannen i ett beslut riktade kritik mot en vårdgivare som ingått avtal med ett företag om journalföring (dnr. 3032-2011). Omständigheterna i ärendet var att läkarsekreterare hos företaget lyssnade av läkardiktat som sedan skrevs ned som en journalanteckning. Justitieombudsmannen konstaterade att läkarsekreterarna hos företaget inte omfattas av den tystnadsplikt enligt offentlighets- och sekretesslagen som gäller för vårdgivarens egen personal. Läkarsekreterarna hade en avtalsreglerad tystnadsplikt i förhållande till arbetsgivaren (dvs. företaget). Vidare följer av regelverket om behandling av personuppgifter en sorts tystnadsplikt för den som behandlar uppgifterna. Enligt Justitieombudsmannen är dessa ”alternativa” tystnadsplikter för läkarsekreterarna inte tillräckliga för att anse att ett utlämnande kan ske utan att det innebär men (skada) för den som skyddas av sekretessen. Vid bedömningen har – mot bakgrund av att de uppgifter som behandlas enligt avtalen är av mycket integritetskänsligt slag – vikt lagts bl.a. vid att vårdgivarens egen personal kan dömas för brott mot tystnadsplikt om en sekretessbelagd uppgift felaktigt röjs, medan så inte är fallet när det gäller läkarsekreterare som är anställda i företaget. Ett utlämnande har inte heller haft stöd i någon sekretessbrytande bestämmelse.

Man bör vara försiktig med att dra alltför långtgående slutsatser utifrån Justitieombudsmannens beslut då användningen av molntjänster typiskt sett inte innebär att anställda hos molntjänstleverantören tar del av kundernas uppgifter på det sätt som skett i det aktuella ärendet. Även om det finns anställda hos molntjänstleverantören som rent tekniskt kan komma åt uppgifterna finns det ofta instruktioner och tekniska åtgärder som begränsar denna åtkomst. Skillnaderna i detta hänseende kan påverka bedömningen. En anställd hos en leverantör som obehörigt skaffar sig tillgång till lagrade uppgifter kan även dömas för dataintrång.

7.2.3 eSams rättsliga uttalande den 23 oktober 2018 (VER 2018:57)

eSams juridiska expertgrupp har tagit fram ett rättsligt uttalande den 23 oktober 2018 (VER 2018:57) beträffande behandling av sekretessreglerade uppgifter i samband med användningen av vissa typer av molntjänster. Uttalandet tar sikte på sådana molntjänster som erbjuds av företag som har servrar i olika länder så att informationen kan finnas sparad i flera länder och snabbt flyttas mellan olika jurisdiktioner samt vara åtkomlig över nät. Internationell rättshjälp är den väg en stat normalt har att gå enligt folkrätten för att få ta del av elektronisk bevisning från andra stater när det gäller innehåll i molnkonton och liknande. Det innebär att den stat som behöver information som finns på en server i en annan stat måste begära hjälp av den andra statens myndigheter för att få ut informationen.

Ett intensivt regelarbete pågår dock i många stater, vilket gör rättsläget osäkert. Det förekommer att företag enligt den rättsordning som gäller i ett annat land är skyldiga att under vissa omständigheter lämna information till en myndighet i det landet utan att frågan hanteras genom internationellt samarbete mellan berörda stater. Ett exempel är den reglering som innebär att amerikanska myndigheter ska ges tillgång även till data som lagras utomlands och att amerikanska tjänsteleverantörer av det skälet inte kan vägra att lämna ut sådana data. Sekretessreglerade uppgifter kan enligt denna reglering komma att lämnas ut även om själva lagringen sker inom EU:s gränser. Enligt eSams juridiska expertgrupp får sekretessreglerade uppgifter anses vara röjda om de lämnas till ett företag som omfattas av en förpliktelse av beskrivet slag.

Det finns dessutom företag som erbjuder molntjänster där ägarförhållandena eller den geografiska placeringen av de tekniska hjälpmedlen är sådana att det finns skäl att ifrågasatta skyddet för mänskliga rättigheter, bland annat skyddet för privatlivet, eller skyddet för det allmännas intressen, t.ex. skyddet för rikets säkerhet. Även här bör enligt eSams juridiska expertgrupp en försiktig bedömning göras. Ger omständigheterna anledning att befara att mänskliga rättigheter eller nationens intressen inte skulle säkerställas om svenska myndigheters data hade tillgängliggjorts får dessa uppgifter anses vara röjda eftersom det inte längre är osannolikt att de lämnas till utomstående.

7.2.4 Juridik som stöd för förvaltningens digitalisering SOU 2018:25

Frågan om sekretessregleringen utgör hinder mot att i vissa fall lämna ut uppgifter som omfattas av sekretess till privata leverantörer i samband med användandet av underleverantörer har lyfts fram i betänkandet Juridik som stöd för förvaltningens digitalisering SOU 2018:25. Detta eftersom osäkerheten kring rättsliga förutsättningar för att använda underleverantörer, särskilt för IT-drift och andra IT-baserade funktioner kan hindra eller hämma digitaliseringen i offentlig sektor.

I utredningen föreslås en i lag reglerad tystnadsplikt för uppgifter som omfattas av sekretess och som lämnas ut till en privat underleverantör när det är fråga om enbart teknisk bearbetning eller lagring. Tystnadsplikten ska gälla för anställda och uppdragstagare hos den privata leverantören. Den föreslagna bestämmelsen om tystnadsplikt är straffsanktionerad.

I utredningen föreslås även en ny sekretessbrytande bestämmelse för att myndigheter i samband med användandet av underleverantörer som enbart genomför teknisk bearbetning eller lagring ska kunna lämna ut sekretessbelagda uppgifter till privata eller offentliga aktörer. Ett sådant sekretessgenombrott får bara ske om uppgiften behövs för att leverantören ska kunna utföra uppdraget. En uppgift får inte heller lämnas ut om övervägande skäl talar för att det intresse som sekretessen ska skydda har företräde framför intresset av att uppgiften lämnas ut eller det av andra skäl är olämpligt.

7.3 Överföring till tredje land

När information lagras i en molntjänst som är baserad utanför EU/EES finns en risk att informationen blir tillgänglig i ett land utanför EU/EES. I och med dataskyddsförordningen har alla EU:s medlemsstater ett likvärdigt skydd för personuppgifter och personlig integritet. Detta omfattar även EES-länderna. Därför bedöms personuppgifter kunna föras över på ett säkert sätt inom detta område. Utanför EU/EES finns däremot inga generella regler som ger motsvarande skydd. Dataskyddsförordningen innehåller därför regler om under vilka förutsättningar det är tillåtet att föra över personuppgifter till länder utanför EU/EES. En överföring av personuppgifter utanför EU/EES är tillåten om det finns ett beslut från EU-kommissionen om att exempelvis ett land utanför EU/EES säkerställer en adekvat skyddsnivå, om den personuppgiftsansvarige har vidtagit lämpliga skyddsåtgärder, till exempel ingått avtal som innehåller standardavtalsklausuler samt i särskilda situationer och i enstaka fall.

Bedömning/Aktivitet
En region bör kravställa att en leverantör som behandlar personuppgifter i tredje land på uppdrag av regionen använder sig av t.ex. standardavtalsklausuler eller är anslutna till Privacy Shield för att uppnå en adekvat skyddsnivå för uppgifterna.

8 Förvaringsrekvisitet för allmänna handlingar enligt 2 kap. 4 § tryckfrihetsförordningen

En allmän handling är i princip tillgänglig för alla att ta del av, om den inte är hemlig på grund av sekretess enligt offentlighets- och sekretesslagen. En handling anses allmän bland annat om den är förvarad hos en myndighet.

Det är något oklart vem som förfogar och bestämmer över uppgifterna som genereras av mätutrustning som tillhandahålls av vårdgivare i hemmet och därmed hos vem uppgifterna är förvarade[42] när de skapas i utrustningen. Å ena sidan borde inte uppgifterna vara tillgänglig för vårdgivaren när de skapas i utrustningen i patientens hem, utan först när de överförs till vårdgivaren. Å andra sidan sker all informationsinsamling enligt vårdgivarens ordination och under vårdgivarens överinseende vilket talar för att uppgifterna får anses förvarade hos en region så snart uppgifterna skapats oavsett om de överförts eller inte.

Bedömning/Aktivitet
En region bör se till att uppgifterna som genereras i mätutrustningen i hemmet, överförs så snabbt som möjligt till regionen för att undvika oklarheter.

9 Patientens privata enhet

Om att ta ställning till hur man ska förhålla sig till de fall där patienten önskar använda en privat enhet.

Det är upp till en region att bestämma huruvida privata enheter ska tillåtas som en del i e-hälsolösningen. Det viktiga i sammanhanget är att säkerställa att dataskyddsförordningens och patientdatalagens krav uppfylls oavsett vilken lösning som nyttjas. Kraven tar sikte på patientuppgifterna i sig, vilket innebär att säkerhetskraven inte nödvändigtvis behöver lösas ut i själv enheten utan kan likväl lösas i appen/webblösningen vilket är lämpligt om patienten ska kunna använda en privat enhet.

[42] Tryckfrihetsförordningen 2 kap 4§

Bilaga 1

Krav som kan användas vid upphandling

Nedan återfinns krav som dels är kopplade till de bedömningar/aktiviteter som anges i bilaga 1 men även generella krav som kan användas i upphandlingen. Utöver dessa krav bör de krav som framkommer via riskanalysen och informationsklassificeringen att tas med i upphandlingen.

Generella krav

1. Leverantören ska följa gällande lagstiftning som är applicerbar på e-hälsolösningen såsom exempelvis dataskyddsförordningen och patientdatalagen.

2. Leverantören ska vid överföring av personuppgifter till tredje land säkerställa en adekvat skyddsnivå genom t.ex. standardavtalsklausuler, anslutning eller Privacy Shield utifrån dataskyddsförordningen.

3. Leverantören ska ha upprättat styrande dokument avseende strategier för skydd och behandling av personuppgifter genom bl.a. skriftliga policys och riktlinjer.

4. Leverantören ska ha upprättade avtal som säkerställer att personal inom organisationen med behörighet att behandla personuppgifter har åtagit sig att iaktta konfidentialitet alternativt att personalen omfattas av lagstadgad tystnadsplikt.

5. Leverantören ska ha tekniska och organisatoriska åtgärder som är utformade för att ge säkert adekvat skydd för personuppgifter.

6. Leverantören ska säkerställa att leverantören som personuppgiftsbiträde inte ingår avtal med ett underbiträde, som ska behandla regionens personuppgifter, utan regionens samtycke. Om sådant samtycke inhämtats ska personuppgiftsbiträdesavtal finnas upprättat mellan parterna i enlighet med dataskyddsförordningen, med samma innehåll som biträdesavtalet mellan Leverantören och Regionen.

7. Leverantören ska säkerställa att personuppgifter inte överförs till tredje land eller en internationell organisation utan samtycke från Regionen.

8. Det ska finnas teknisk möjlighet till att rätta och radera personuppgifter i det system som tillhandahålls. Det ska också finnas teknisk möjlighet att ta fram ett registerutdrag.

9. Leverantören ska se till att möjlighet till begränsning av behandling av personuppgifter finns i det system som tillhandahålls.

10. Leverantören ska ha en upprättad och dokumenterad rutin för hantering av personuppgiftsincidenter för vidare rapportering till personuppgiftsansvarig.

Detaljerade krav

11. E-hälsolösningen bör logga samtliga åtgärder som har vidtagits med patientuppgifterna. Utöver det bör även användaridentitet, patientidentitet och tidpunkt samt vårdenhet loggas.

12. Systemets loggar bör kunna exporteras till en texteditor.

13. Överföring av patientuppgifter från e-hälsolösningen bör göras på ett sådant sätt, t.ex. via kryptering, att ingen obehörig kan ta del av uppgifterna.

14. Stark autentisering bör användas för åtkomst till patientuppgifter för både användare och patient. Med stark autentisering menas tvåfaktorsautentisering/autentisering som innebär att identiteten kontrolleras på två olika sätt.

15. Det bör gå att rätta eller förstöra/radera patientuppgifter i e-hälsolösningen.

16. E-hälsolösningen bör kunna hantera signering av journaluppgifter och bekräftelse av åtgärder som rör patientens vård och behandling.

17. E-hälsolösningen bör stödja olika behörighetsnivåer för olika roller av användare genom integration med katalogtjänst såsom AD och HSA-katalog.

18. Det bör vara möjligt att ge varje enskild användare ett personligt inlogg.

19. Varje personligt inlogg bör bestå av en roll och en vårdenhet (verksamhetsuppdrag) vilket styr vad personen får se och kan göra i e-hälsolösningen.

20. Det bör finnas funktion för "aktiva val" för åtkomst av patientuppgifter inom vårdgivaren, det vill säga att patientuppgifterna tillgängliggörs stegvis, baserat på den information användaren behöver.

21. Det bör i systemet finnas en funktionalitet för spärrhantering.

22. Teknisk funktionalitet i systemet bör finnas för att öppna ovanstående spärr med samtycke ifrån patienten.

23. Teknisk funktionalitet i systemet bör finnas för att öppna ovanstående spärr vid nödöppning av valda patientuppgifter.

24. Det bör finnas funktion för "aktiva val" för åtkomst av patientuppgifter mellan vårdgivarna, det vill säga att patientuppgifterna tillgängliggörs stegvis, baserat på den information användaren behöver.

25. Det bör framgå om det finns ospärrade uppgifter hos en annan vårdgivare.

26. Det bör i e-Hälsolösningen finnas en funktionalitet för spärrhantering mellan vårdgivarna. Om en patient har motsatt sig att hans eller hennes patientuppgifter görs tillgängliga för den som arbetar hos en annan vårdgivare, bör det framgå av dokumentationen att det finns spärrade patientuppgifter.

27. Teknisk funktionalitet i systemet bör finnas för att öppna ovanstående spärr vid nödöppning av valda patientuppgifter.