Personcentrerad data och juridik

En delrapport inom SWEPER-projektet

NOVEMBER 2018

VÅRDEN BLIR ALLTMER KOMPLEX och individuellt anpassad efter den enskilda patientens förutsättningar och behov.

Det innebär stora möjligheter att optimera varje patients behandling, men ställer också ökade krav på diagnostik, behandling och uppföljning.

Mängden data om varje individ växer snabbt. Det kan vara den information som patienten ger vid besök inom vården – exempelvis all data som ett vanligt blodprov kan ge – men också data som individen själv producerar, exempelvis genom hälsoappar. All data om individen som har betydelse för välbefinnandet kan kallas för *systematiska hälsodata*.

Rätt använd skulle den systematiska hälsodatan som finns kunna användas för att ge en hälso- och sjukvård specialanpassad för var och en av oss, så kallad *precisionsmedicin*. Individen skulle också kunna använda dessa data för *precisionshälsa*.

Vården behöver kunna följa en rad olika sekventiellt insatta behandlingar och utvärdera användningen av såväl diagnostiska och kirurgiska metoder på ett mer systematiskt sätt än vad som sker i dag. Patienternas bidrag med information kring sin hälsa är också en viktig komponent i uppföljningen. Dessutom börjar nu många mediciner inom exempelvis cancerområdet att breddanvändas, med indikationer mer baserade på vilka genetiska förändringar som tumören har, än på diagnos.

SWEPER är ett nationellt initiativ som vill förbättra och stödja möjligheterna för life science-sektorn i Sverige att få tag i och använda data. Många av dessa lösningar kommer att kunna bidra till det vi kallar precisionsmedicin, men även kunna bidra till precisionshälsa.

Syftet med SWEPER-projektet är att

- utveckla vården, bidra till forskning och ökad kunskap för att kunna använda de behandlingsmetoder vi har på rätt individer, samt att
- generera en bas för nya innovationer och translation från ett kunskapsområde till ett annat, genom interaktion mellan vård, akademi och industri.

Denna analys är en del av ett delprojekt inom SWEPER som ska sammanfatta, diskutera och lyfta problem med gällande personuppgifts–lagstiftning för att vägleda framväxten av nya lösningar inom precisionsmedicin och databehandling.

Denna juridiska analys har till syfte att komplettera Manolis Nymarks rapport Laglighetsprövning av realtidsregister inom cancervården *för att tydliggöra vad som gäller utifrån den nya dataskydds-förordningen och andra lagändringar som skett utifrån denna förordning.*

Analysen ska också sammanställa underlag och lagstiftning för att tydliggöra möjliga juridiska angreppssätt. Därmed ska den kunna användas som stöd för att ta fram plattformslösningar som innehåller stora mängder personuppgifter, inklusive känsliga sådana, som ska behandlas för flera olika ändamål.

Under rubrikerna Framtidsdiskussion *lyfts idéer och tankar hur tillgången till patientuppgifter och data skulle kunna underlättas om lagstiftningen ändrades ifrån dagens reglering. Det har dock inte koppling till pågående lagstiftningsarbete utan är till för att väcka diskussion och tankar.*

Sammanfattning

Dataskyddsförordningen är till stor del lik *person-uppgiftslagen*.

Några nyheter är

- personuppgiftsincidenter
- konsekvensbedömningar
- sanktionsavgifter
- dataportabilitet
- uppförandekoder
- certifieringar
- att personuppgiftsansvariga ska kunna visa på efterlevnad.

Denna förordning har resulterat i att Sverige fått en *dataskyddslag*. *Patientdatalagen* har ändrats marginellt av dataskyddsförordningen. Något som redan fanns tidigare är begränsningen i patient-datalagen vad som ska och får journalföras, vilket kan begränsa möjligheten att insamla en stor mängd data från patienterna. Dataskyddsförord-ningen påverkar dock inte tidigare legala bedömn-ing i *Laglighetsprövning av realtidsregister inom cancervården*, Manolis Nymark 2017.

Mycket går att göra i dag, men lagstiftningen gör ibland att det blir komplext och krångligt. I denna analys har flera förutsättningar och möjligheter för att hantera personuppgifter – på en och samma eventuella plattformslösning till-hörande flera olika personuppgiftsansvariga – lyfts fram.

KORTFATTAT

- Samtliga personuppgifts-ansvariga måste vara utpekade och dessa måste ha en rättslig grund för att behandla personuppgifterna med fastställda ändamål.
- Informationen ska vara logiskt åtskild.
- Vårdgivarna skulle kunna dela information med stöd av regelverket för samman-hållen journalföring eller digitalt utlämnande.
- Vårdgivarna skulle kunna överföra uppgifter till nationella kvalitetsregister.
- Patienten skulle under vissa förutsättningar kunna bidra till journal och kvalitets-register.
- Uppgifter skulle kunna lämnas ut av vårdgivarna för forskning, eventuellt via ett personuppgiftsbiträde.
- Patienten skulle kunna ha en egen area för hälsodata mm under vissa förutsättningar.

CHECKLISTA FÖR DATASKYDDSFÖRORDNINGEN

Dataskyddsförordningen (GDPR) gäller i hela EU. Den har till syfte att skapa en enhetlig och likvärdig nivå för skyddet av personuppgifter. Dataskyddsförordningen består av 99 artiklar och 173 beaktandesatser (skäl).

För att uppfylla kraven i dataskyddsförordningen behöver samtliga artiklar omhändertas, men nedan återfinns en kort checklista över vad man behöver göra och tänka på inför behandling av personuppgifter.

- ☐ Säkerställ ändamål och vem eller vilka som är personuppgiftsansvariga. Om det föreligger ett gemensamt personuppgiftsansvar behöver ansvaret tydliggöras mellan de personuppgiftsansvariga.
- ☐ Utred vilken eller vilka rättsliga grunder som finns för att behandla personuppgifterna. Tänk då på att vissa rättsliga grunder är lämpligare än andra. Det är också så att de registrerades rättigheter varierar beroende på vilken rättslig grund som finns.
- ☐ Tänk till kring uppgiftsminimeringsprincipen och lagringsminimeringsprincipen. Vilka personuppgifter behövs för att uppnå syftet med behandlingen? Hur länge behövs personuppgifterna? Observera att det kan finnas bevarandekrav utifrån annan lagstiftning, till exempel *arkivlagen*.
- ☐ De registrerade har rätt till omfattande information innan personuppgifterna behandlas. Därför är det viktigt att tänka på vilka kategorier av registrerade som behandlas och hur de på bästa sätt kan tillgängliggöra sig denna information.
- ☐ För att skydda personuppgifterna behöver det analyseras vilken typ och nivå av skydd som behövs. Detta kan man göra genom att exempelvis genomföra informationsklassificeringar och riskanalyser. Vidtagna säkerhetsåtgärder behöver sedan följas upp och utvärderas så att adekvat skydd finns med under hela livscykeln för personuppgifterna.
- ☐ Om någon annan behandlar personuppgifter på uppdrag av den eller de personuppgiftsansvariga, så behöver ett personuppgiftsbiträdesavtal tecknas. Det reglerar hur exempelvis underleverantören får behandla personuppgifterna.

Dataskyddsförordningen

Dataskyddsförordningen (GDPR, The General Data Protection Regulation) gäller sedan 25 maj 2018 i hela EU. Den har till syfte att skapa en enhetlig och likvärdig nivå för skyddet av personuppgifter så att det fria flödet av uppgifter inom Europa inte hindras. Mycket i dataskyddsförordningen liknar de regler som fanns i personuppgiftslagen som numera är upphävd, men det finns en del nyheter.

Dataskyddsförordningen gäller i princip för all automatiserad behandling av personuppgifter och i vissa fall även manuell behandling av personuppgifter. Personuppgifter är varje upplysning som avser en identifierad eller identifierbar fysisk person. Avgörande är att uppgiften – enskilt eller i kombination med andra uppgifter – kan knytas till en levande person. Personuppgifter om barn anses särskilt skyddsvärda i dataskyddsförordningen, eftersom barn kan ha svårare att förutse riskerna med att lämna ifrån sig uppgifter och att förstå vilken rätt till skydd för sina uppgifter som de har.

I Sverige har vi med personuppgiftslagen tidigare haft den så kallade *missbruksregeln* som innebär enklare regler för personuppgifter i ostrukturerat material. Den är numera borttagen och all personuppgiftsbehandling regleras på samma sätt oavsett om personuppgifterna är strukturerade eller inte.

Dataskyddsförordningen gäller för personuppgiftsbehandling som har anknytning till EU, antingen när den som behandlar personuppgifterna är etablerad inom EU eller då någon utanför EU erbjuder tjänster och varor till personer inom unionen eller övervakar deras beteenden här.

Rättslig grund

All personuppgiftbehandling måste ha en rättslig grund för att vara tillåten. En personuppgiftsbehandling enligt dataskyddsförordningen är därför endast tillåten om det finns en rättslig grund. Det kan dock finnas flera möjliga grunder att använda för en personuppgiftsbehandling men då ska den som är bäst lämpad användas. För offentlig sektor aktualiseras främst de rättsliga grunderna

- avtal
- rättslig förpliktelse
- uppgift av allmänt intresse eller myndighetsutövning.

Privata aktörer bör främst använda sig av

- samtycke
- avtal
- rättslig förpliktelse
- intresseavvägning.[1]

De olika rättsliga grunderna medför olika rättigheter för de registrerade och skyldigheter för de personuppgiftsansvariga. För de rättsliga grunderna avtal och samtycke aktualiseras rätten att bli glömd och rätten till dataportabilitet. Enligt Datainspektionen är det också i många fall inte lämpligt att använda sig av den rättsliga grunden samtycke.[2] Det beror dels på de krav som ställs på själva samtycket, dels att samtycket när som helst kan tas tillbaka av den registrerade. Om det

1 https://www.datainspektionen.se/lagar--regler/dataskydds-forordningen/rattslig-grund/
2 https://www.datainspektionen.se/lagar--regler/dataskydds-forordningen/rattslig-grund/

De rättsliga grunderna i dataskyddsförordningen.

FRAMTIDSDISKUSSION

GENERELLA SAMTYCKEN

Att ett samtycke ska vara specifikt och informerat medför att ett generellt samtycke för exempelvis all slags forskning nu och i framtiden inte kan lämnas av en registrerad. Detta är alltså inte möjligt med dagens lagstiftning men det skulle kunna underlätta tillgången till patientuppgifter för till exempel syftet forskning. För att underlätta tillgången till data kan man tänka sig ett nationellt samtyckesregister som både personer och system/maskiner skulle kunna använda sig av, som skulle gälla för all typ av forskning, system för sammanhållen journalföring och så vidare, såtillvida att individen inte tagit tillbaka sitt samtycke eller aldrig lämnat något.

Detta skulle givetvis underlätta hanteringen och patienterna skulle inte behöva tillfrågas gång på gång för att inhämta olika typer av samtycke för olika situationer och ändamål.

Lösningen skulle kunna innebära en påverkan på den personliga integriteten beroende på hur regelverket kring det nationella samtyckesregistret skulle utformas. Men detta är som sagt inte en framkomlig väg utifrån dagens lagstiftning.

är möjligt att välja en annan rättslig grund än samtycke så är det alltså att föredra.

SAMTYCKE

Myndigheter avråds i dataskyddsförordningen från att använda samtycke som grund för sina behandlingar eftersom det oftast råder ett ojämlikt förhållande mellan en myndighet och en enskild registrerad.[3] Dessutom är samtycke en mycket osäker grund då samtycke när som helst kan tas tillbaka av den registrerade.

Ett samtycke ska vara frivilligt, specifikt och informerat.[4] Det får heller inte föreligga ojämlikt maktförhållande mellan den som efterfrågar ett samtycke och den som ska lämna det.

Datainspektionen har gett som exempel att samtycke till exempel kan användas när en nämnd planerar vägarbeten och att invånare kan anmäla sig för att få uppdateringar av informationen via e-post.[5]

FULLGÖRA ETT AVTAL MED DEN REGISTRERADE

För att denna rättsliga grund ska användas ska behandlingen vara nödvändig för att fullgöra ett avtal med den registrerade eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås. Denna rättsliga grund kan till exempel användas för behandling av en arbetstagares personuppgifter om det är nödvändigt för att anställningsavtalet eller något annat avtal mellan arbetsgivaren och arbetstagaren ska kunna uppfyllas.

RÄTTSLIG FÖRPLIKTELSE

Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse för den personuppgiftsansvarige. När det gäller detta ändamål får medlemsstaterna – till exempel Sverige – behålla eller införa mer specifika bestämmelser genom att fastställa specifika krav för uppgiftsbehandlingen och andra åtgärder för att säkerställa en laglig och rättvis behandling.

Här ska alltså nationell lagstiftning komplettera bestämmelserna i dataskyddsförordningen. Dessutom måste den rättsliga förpliktelsen i sig vara tillräckligt tydlig när det gäller den behandling av personuppgifter som krävs. Exempel på rättslig förpliktelse är journalföring utifrån bestämmelserna i patientdatalagen.

SKYDDA VITALA INTRESSEN

Denna rättsliga grund ska användas om behandlingen är nödvändig för att skydda den registrerades vitala intressen.

Behandling av personuppgifter på denna rättsliga grund bör i princip endast äga rum om behandlingen inte uppenbart kan ha en annan rättslig grund. Exempel på intressen som är av grundläggande betydelse för den registrerade är till exempel när behandlingen är nödvändig av humanitära skäl, bland annat

- för att övervaka epidemier och deras spridning
- i humanitära nödsituationer, särskilt vid naturkatastrofer eller katastrofer orsakade av människan.

UPPGIFT AV ALLMÄNT INTRESSE

För att använda denna grund ska behandlingen vara nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i utförande av myndighetsutövning.

I dataskyddsutredningen framgår bland annat att man bör kunna utgå ifrån att de obligatoriska uppgifter som utförs av kommuner och landsting, till följd av deras åligganden enligt lag eller förordning, är av allmänt intresse. Begreppet *uppgifter av allmänt intresse* omfattar dock inte bara sådant som utförs som en följd av ett uttryckligt åliggande eller uppdrag. Den personuppgiftsansvarige behöver inte vara skyldig att utföra uppgiften för att den lagliga grunden allmänt intresse ska kunna

3 Dataskyddsförordningen beaktandesats 43
4 Dataskyddsförordningen beaktandesats 32
5 https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/rattslig-grund/samtycke/

användas. Däremot måste behandlingen vara *nödvändig*.[6]

INTRESSEAVVÄGNING

Behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges berättigade intressen.

En nyhet med dataskyddsförordningen är att den rättsliga grunden ”den personuppgiftsansvariges berättigade intresse”, också kallad ”intresseavvägning” numera inte får användas för behandling som utförs av offentliga myndigheter när de fullgör sina uppgifter. Intresseavvägning innebär att man ska väga den registrerades intresse att inte få sina personuppgifter behandlade mot den personuppgiftsansvarigas intresse att behandla dem.

Här är en möjlig tolkning att myndigheter inte får använda sig av den rättsliga grunden intresseavvägning när de utför sina officiella uppdrag (kärnverksamhet), men att intresseavvägning fortfarande kan användas som grund för behandling rörande mindre viktiga behandlingar utan direkt koppling till myndighetens officiella uppdrag.

Exempel på sådan behandling skulle kunna vara

- löne-, utvecklings- och utvärderingssamtal
- behörighetssystem
- vissa kvalitetsmätningar inom myndigheten.

Datainspektionen har dock inte tagit något klart ställningstagande i frågan vilket medför att rättsläget får anses något oklart.

Registrerades rättigheter

Något som är förändrat är informationsplikten till de registrerade. Även tidigare har det funnits en plikt att informera de registrerade, men med dataskyddsförordningen har denna skyldighet utökats och förtydligats.

6 Prop. 2017/18:105 s 55 ff

FRAMTIDSDISKUSSION

DATAPORTABILITET

Om rätten till dataportabilitet inte bara skulle vara kopplad till dagens två rättsliga grunder, utan istället till samtliga rättsliga grunder, och samtidigt även omfatta alla personuppgifter som en personuppgiftsansvarig behandlar, så skulle man kunna tänka sig att exempelvis patienter på ett smidigare sätt skulle kunna byta vårdgivare. Detta skulle ske utan att förlora viktig historik.

Man skulle också kunna tänka sig att patienten smidigare skulle kunna använda sig av personuppgifterna, för att exempelvis kunna nyttja olika digitala hälso- och sjukvårdstjänster i andra delar av världen.

Utöver rätt till information har den registrerade även rätt till

- registerutdrag
- rättelse
- att bli bortglömd
- begränsning
- dataportabilitet
- att göra invändningar
- att lämna klagomål
- (i vissa fall) skadestånd.

Den enskilde har också rätt att inte bli föremål för ett beslut som enbart grundas på någon form av automatiserat beslutsfattande – inbegripet profilering – om beslutet kan ha rättsliga följder för den enskilde eller på liknande sätt i betydande grad påverkar honom eller henne. Det finns dock vissa undantag ifrån denna rättighet till exempel i förvaltningslagen.[7]

Rättigheterna är inte absoluta, utan vissa av dem är enbart kopplade till vissa rättsliga grunder i dataskyddsförordningen, såsom rätten att bli glömd och rätten till dataportabilitet. Det innebär att det enbart är för de rättsliga grunderna samtycke och fullgörande av avtal som rätten att bli glömd och rätten till dataportabilitet aktualiseras.

De rättigheter som är nyheter i dataskyddsförordningen är rätt till begränsning, rätt till dataportabilitet och rätten att inte bli föremål för ett beslut som enbart grundas på någon form av automatiserat beslutsfattande.

Rätt till begränsning innebär att uppgifterna markeras så att dessa i framtiden endast får behandlas för vissa avgränsade syften. Rätten till begränsning gäller bland annat när den registrerade anser att uppgifterna är felaktiga och begärt rättelse.

Rätt till dataportabilitet innebär att den som har lämnat sina personuppgifter i vissa fall har rätt att få ut och använda sina personuppgifter på annat håll till exempel i en annan social medietjänst. Den som har tagit emot personuppgifterna är skyldig att underlätta en sådan överflyttning av personuppgifter.

Automatiserat beslutsfattande kan till exempel vara ett automatiserat avslag på en kreditansökan på internet eller vid ett nekande besked från e-rekrytering via internet utan personlig kontakt. Automatiserat beslutsfattande kan vara tillåtet om det är nödvändigt för ingående eller fullgörande av ett avtal mellan den registrerade och den personuppgiftsansvarige eller om den enskilde har gett sitt uttryckliga samtycke.

I dag omfattas oftast inte offentliga aktörer av rätten till dataportabilitet eftersom de till stor del bör använda sig av den rättsliga grunden uppgift av allmänt intresse eller myndighetsutövning och inte samtycke eller avtal.

7 https://skl.se/download/18.2e148555164fd471ee2a7fe/1533301802437/automatiserat%20beslutsfattande.2.0.18maj.pdf

FRAMTIDSDISKUSSION

UPPGIFTSMINIMERINGSPRINCIPEN

Uppgifts- och lagringsminimerings-principerna är liksom övriga delar av dataskyddsförordningen till för att skydda den personliga integriteten. Det kommer dock inom kort bli allt vanligare med nyttjande av *Big data* och avancerade analysverktyg inom hälso- och sjukvården. Dels för att utreda och ställa diagnos, dels för att kunna ge en individanpassad vård och behandling.

Utgångspunkten för detta är att samla på sig stora mängder data som sedan tillsammans kan analyseras på olika sätt och för olika syften. Detta rimmar dock illa med just uppgiftsminimeringsprincipen och lagringsminimeringsprincipen. Uppräkningen av personuppgifter som ska ingå i exempelvis journalen (Patientlagen 3 kap) begränsar just möjligheten att samla på sig en stor mängd data utan att i förväg veta nyttan av denna information. En framgångsfaktor är att faktiskt tänka bredare ifrån början och verkligen analysera vilka personuppgifter som behövs för att uppnå ändamålet med analysen. På så sätt tydliggörs behovet av den stora mängden personuppgifter som behövs så att uppgiftsminimeringsprincipen uppfylls.

Uppgifts- och lagringsminimerings-principen

I och med dataskyddsförordningen har två principer förtydligats: uppgiftsminimeringsprincipen och lagringsminimeringsprincipen.

Uppgiftsminimeringsprincipen innebär att personuppgifterna som behandlas ska vara adekvata, relevanta och inte för omfattande i förhållande till ändamålet. Det innebär alltså att man inte får behandla personuppgifter som inte behövs för att uppnå ändamålet med person-uppgiftbehandlingen.

Lagringsminimeringsprincipen innebär att man bara får spara personuppgifter så länge som de behövs för ändamålet med personuppgifts-behandlingen. I vissa fall behöver dock uppgifter-na bevaras utifrån annan lagstiftning, till exempel arkivlagen.

Känsliga personuppgifter

Vissa personuppgifter är till sin natur särskilt känsliga och har därför ett starkare skydd. De kallas för känsliga personuppgifter.

Känsliga personuppgifter är uppgifter om ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i en fack-förening, hälsa, en persons sexualliv eller sexuella läggning, genetiska uppgifter eller biometriska uppgifter som entydigt identifierar en person.

Myndigheter får behandla personuppgifter som rör lagöverträdelser. Andra än myndigheter måste ha stöd i föreskrifter eller särskilda beslut för att få behandla sådana uppgifter.

Personnummer och samordningsnummer får behandlas om de registrerade har gett sitt samtycke. Finns det inget samtycke får person-nummer behandlas bara när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl.

När känsliga personuppgifter ska samlas in och behandlas är det alltså viktigt att tänka på vilket stöd som finns för denna behandling. Känsliga personuppgifter kräver också ofta annan typ av skydd än personuppgifter som inte tillhör dessa särskilda kategorier.

Uppförandekod och certifiering

En nyhet är att det inte längre är tillräckligt att följa lagen, utan den som är ansvarig för person-uppgiftsbehandlingen måste också kunna visa att och hur man följer bestämmelserna i dataskydds-förordningen.

Personuppgiftsansvariga kan göra detta på olika sätt, bland annat genom att certifiera sig eller följa en godkänd uppförandekod.

En *uppförandekod* är en uppsättning riktlinjer som bidrar till att de företag eller organisationer som har anslutit sig till koden tillämpar reglerna i dataskyddsförordningen korrekt. Utfärdandet av en certifiering ska göras av ett ackrediterat certifieringsorgan. Det är ännu inte beslutat vem som ska utfärda ackrediteringar, men det kommer antingen att vara Datainspektionen eller det nationella ackrediteringsorganet Swedac. Hur certifieringar kommer att gå till är ännu inte klart.

Inbyggt dataskydd och dataskydd som standard

Inbyggt dataskydd (*privacy by design*) innebär att man tar hänsyn till integritetsskyddsreglerna redan när man utformar IT-system och rutiner och fortsätter beakta dessa under person-uppgifternas hela livscykel. Ett sätt att beakta detta är att kontinuerligt genomföra informations-klassificeringar, riskanalyser och att vidta åtgärder utifrån dessa. Inbyggt dataskydd är ett sätt att se till att kraven i dataskyddsförordningen uppfylls och att den registrerades rättigheter skyddas.

Kravet på dataskydd som standard (*privacy by default*) innebär i korthet att den som behandlar personuppgifter ska se till att personuppgifter i standardfallet inte behandlas i onödan. Det kan till exempel handla om att de förvalda inställningarna i en tjänst för sociala media är satta så att inte mer

information än nödvändigt samlas in, delas ut eller visas.

Personuppgiftsbiträden

Dataskyddsförordningen innehåller särskilda skyldigheter för de som behandlar personuppgifter.

En nyhet i dataskyddsförordningen är att många av de skyldigheter som tidigare har gällt för den personuppgiftsansvarige nu även gäller för personuppgiftsbiträdet. De biträden som den personuppgiftsansvarige anlitar ska kunna ge tillräckliga garantier för att behandlingen uppfyller kraven i dataskyddsförordningen och säkerställer att den registrerades rättigheter skyddas. Några av de skyldigheter som bara har gällt för den personuppgiftsansvarige men som nu även gäller för personuppgiftsbiträdet, är till exempel

- kraven på att föra register över behandlingar
- att säkerställa en lämplig säkerhetsnivå
- att i vissa fall utse ett dataskyddsombud.

Även personuppgiftsbiträdet kan bli föremål för tillsyn eller administrativa sanktionsavgifter och bli skadeståndsansvarig.

Personuppgiftsincidenter

För att följa dataskyddsförordningen är det viktigt att organisationer som behandlar personuppgifter har rutiner på plats för att kunna upptäcka, rapportera och utreda personuppgiftsincidenter. Det krävs både organisation och teknik, dels för att upptäcka incidenten, dels för hanteringen för att anmäla detta till Datainspektionen.

En personuppgiftsincident är en säkerhetsincident som kan innebära risker för människors friheter och rättigheter. Exempel på personuppgiftsincidenter är om en eller flera personuppgifter har blivit förstörda, gått förlorade på annat sätt eller kommit i orätta händer. I vissa fall måste även personuppgiftsincidenten anmälas till Datainspektionen och till de registrerade.

Konsekvensbedömningar

En annan nyhet i dataskyddsförordningen är att man måste göra en konsekvensbedömning om man planerar för att genomföra en personuppgiftsbehandling med hög risk för de registrerade. Konsekvensbedömningen är en process för att ta reda på vilka risker som finns med att behandla personuppgifter, ta fram rutiner och åtgärder för att bemöta dessa risker och för att visa att man uppfyller dataskyddsförordningens krav. Om det efter en konsekvensbedömning fortfarande finns hög risk med personuppgiftsbehandlingen ska samråd med Datainspektionen ske innan behandlingen påbörjas.

Datainspektionen ska upprätta och offentliggöra en förteckning över det slags behandlingsverksamheter som omfattas av kravet på en konsekvensbedömning avseende dataskydd. Datainspektionen har angett att de kommer att göra en sådan förteckning.

Sanktionsavgifter

Datainspektionen kan besluta om en administrativ sanktionsavgift om regelverket i dataskyddsförordningen inte följs.

KORTFATTAT

- Dataskyddsförordningen har medfört nya lagkrav, men dessa bedöms inte i sak förändra rättsläget som Manolis Nymark redogör för i *Laglighetsprövning av realtidsregister inom cancervården*.
- Däremot måste personuppgiftsansvariga se till att de följer regelverket i dataskyddsförordningen, både det regelverk som fanns redan i personuppgiftslagen, men även för de nyheter som kommit via dataskyddsförordningen.

Patientdatalagen

Patientdatalagen innehåller bestämmelser om behandling av personuppgifter som främst avser enskilda patienter inom hälso- och sjukvården inklusive tandvården. Lagen gäller för alla vårdgivare oavsett om verksamheten bedrivs i privat eller offentlig regi.

Något som varit och är problematiskt med patientdatalagen är definitionen på vårdgivare eller framförallt de konsekvenser definitionen medför. Ett landsting har till exempel ett ansvar att erbjuda en god hälso- och sjukvård, vilket kan ske genom att teckna vårdavtal med privata vårdgivare. Landstinget har dock begränsade möjligheter att följa upp den vård som ges hos den privata vårdgivaren utifrån regelverket i patientdatalagen och offentlighets- och sekretesslagen.

Patientdatalagen har varit gällande lag sedan 2008, men i och med dataskyddsförordningens tillkomst har speciallagstiftningar och registerlagstiftningar såsom patientdatalagen behövts ses över.

Av ändringarna i patientdatalagen framgår att patientdatalagen kompletterar dataskyddsförordningen och Sveriges dataskyddslag. Det framgår också att vårdgivare och nationella kvalitetsregister får behandla känsliga personuppgifter får med stöd av artikel 9.2 h i dataskyddsförordningen. Däremot är patientdatalagen inte tillämplig på rättspsykiatrisk vård i de fall behandlingen rör verkställighet av en påföljd då brottsdatalagen istället ska användas.

I kapitlet för nationella kvalitetsregister har regelverket för vilket information som ska lämnas till patienten förändrats. Det hör samman med att patientdatalagen kompletterar dataskyddsförordningen och att lagstiftaren inte sett samma behov av att reglera informationsplikten i patientdatalagen utifrån det regelverk som finns i dataskyddsförordningen. Förändringen i patientdatalagen innebär alltså inte att omfattningen och innehållet i informationen som ska lämnas till patienten har reducerats, utan att delar av regelverket har tagits bort då detta regleras i dataskyddsförordningen.

KORTFATTAT

- Patientdatalagen innehåller få förändringar som genomförts utifrån tillkomsten av dataskyddsförordningen. De förändringar som har skett i patientdatalagen har i princip inte förändrat vårdgivares möjligheter att behandla personuppgifter.
- Patientdatalagens regelverk kan dock tillsammans med uppgiftsminimeringsprincipen och lagringsminimeringsprincipen påverka möjligheten för vårdgivare att samla på sig stora mängder personuppgifter som inte vid insamlandet har ett tydligt ändamål och syfte.

FRAMTIDSDISKUSSION

PERSONUPPGIFTSANSVARIG

Både utifrån dataskyddsförordningen och personuppgiftslagen är det grundläggande att utreda vem eller vilka som är personuppgiftsansvariga för en personuppgiftsbehandling och att dessa har stöd för att genomföra dessa personuppgiftsbehandlingar.

Man kan antingen tänka sig en plattform där respektive vårdgivare behandlar personuppgifter som personuppgiftsansvariga och att dessa via plattformen utlämnar patientinformation till kvalitetsregister och forskningsstudier. Men man kan också tänka sig en plattform som en personuppgiftsansvarig ansvarar för och att alla vårdgivare lämnar ut personuppgifter till den personuppgiftsansvariga för plattformen. Detta är en utmaning, dels utifrån att vårdgivarna ska ha stöd att utlämna personuppgifterna utifrån offentlighets- och sekretesslagen, dels att den som är personuppgiftsansvarig för plattformen ska ha en legal rätt att behandla de personuppgifter som lagras på plattformen.

Lagstiftning forskning

I samband med dataskyddsförordningen har frågan lyfts om det skulle tillskapas en forskningsdatalag för att reglera personuppgiftsbehandling inom forskning. Regeringen har dock bedömt att det för närvarande är tillräckligt att etikprövningslagen och de befintliga registerförfattningarna på forskningsområdet anpassas till dataskyddsförordningen. Det har därför inte tillkommit en forskningsdatalag.

Lagen om etikprövning

Lagen om etikprövning ändras den 1 januari 2019. En ändring är att de sex regionala etikprövningsnämnderna ska avvecklas och att etikprövning av forskning som avser människor istället ska hanteras av en ny myndighet, Etikprövningsmyndigheten.

Etikprövningsmyndigheten ska vara indelad i verksamhetsregioner. Varje verksamhetsregion ska ha en eller flera avdelningar. En avdelning ska pröva ärenden inom vissa forskningsområden.

Utifrån dataskyddsförordningen föreslår regeringen att bestämmelsen som definierar behandlingen av personuppgifter i etikprövningslagen, ska ersättas med en hänvisning till artikel 4.2 i dataskyddsförordningen.

Etikprövningslagen ska tillämpas på forskning som innefattar behandling av:

- personuppgifter som avses i artikel 9.1 i EU:s dataskyddsförordning (personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning, det vill säga känsliga personuppgifter)
- personuppgifter om lagöverträdelser som innefattar brott, domar i brottmål, straffprocessuella tvångsmedel eller administrativa frihetsberövanden.

Enligt utkastet på lagrådsremiss behövs inga ytterligare anpassningar göras i etikprövningslagen och lagändringarna föreslås träda i kraft den 1 januari 2019.

Fram till dess är de övergångsbestämmelser som har föreslagits i propositionen till en ny dataskyddslag av betydelse. De innebär att personuppgiftslagen fortsatt ska gälla efter den 25 maj 2018 i den utsträckning som det i en annan lag eller en förordning finns bestämmelser som innehåller hänvisningar till personuppgiftslagen. Sådana hänvisningar finns i lagen om rättspsykiatriskt forskningsregister, etikprövningslagen och lagen om vissa register för forskning om vad arv och miljö betyder för människors hälsa. Från 25 maj 2018 fram till dess att ändringarna i dessa lagar träder i kraft kommer således bestämmelserna i personuppgiftslagen fortsatt att gälla vid behandling av personuppgifter som omfattas av dessa lagar.

KORTFATTAT

- De förändringar som föreslås ske i lagen om etikprövning bedöms inte påverka de legala förutsättningarna som redogörs för i dokumentet *Laglighetsprövning av realtidsregister inom cancervården*.

FRAMTIDSDISKUSSION

GRÄNSDRAGNINGAR

En frågeställning som blivit allt tydligare efter dataskyddsförordningens tillkomst är just gränsdragningen mellan de etiska frågeställningarna i etikprövningen och ställningstagandet om integritetsskyddet via dataskyddsförordningen är omhändertaget.

Det finns en viss risk att de forskare som fått ett beslut ifrån etikprövningsmyndigheten upplever att de även fått ett godkännande utifrån dataskyddslagstiftningens krav.

Det medför då också frågeställningen om Etikprövningsmyndigheten har mandat att uttala sig om personuppgiftsbehandlingar och vilken roll Datainspektionen i så fall har i dessa sammanhang.

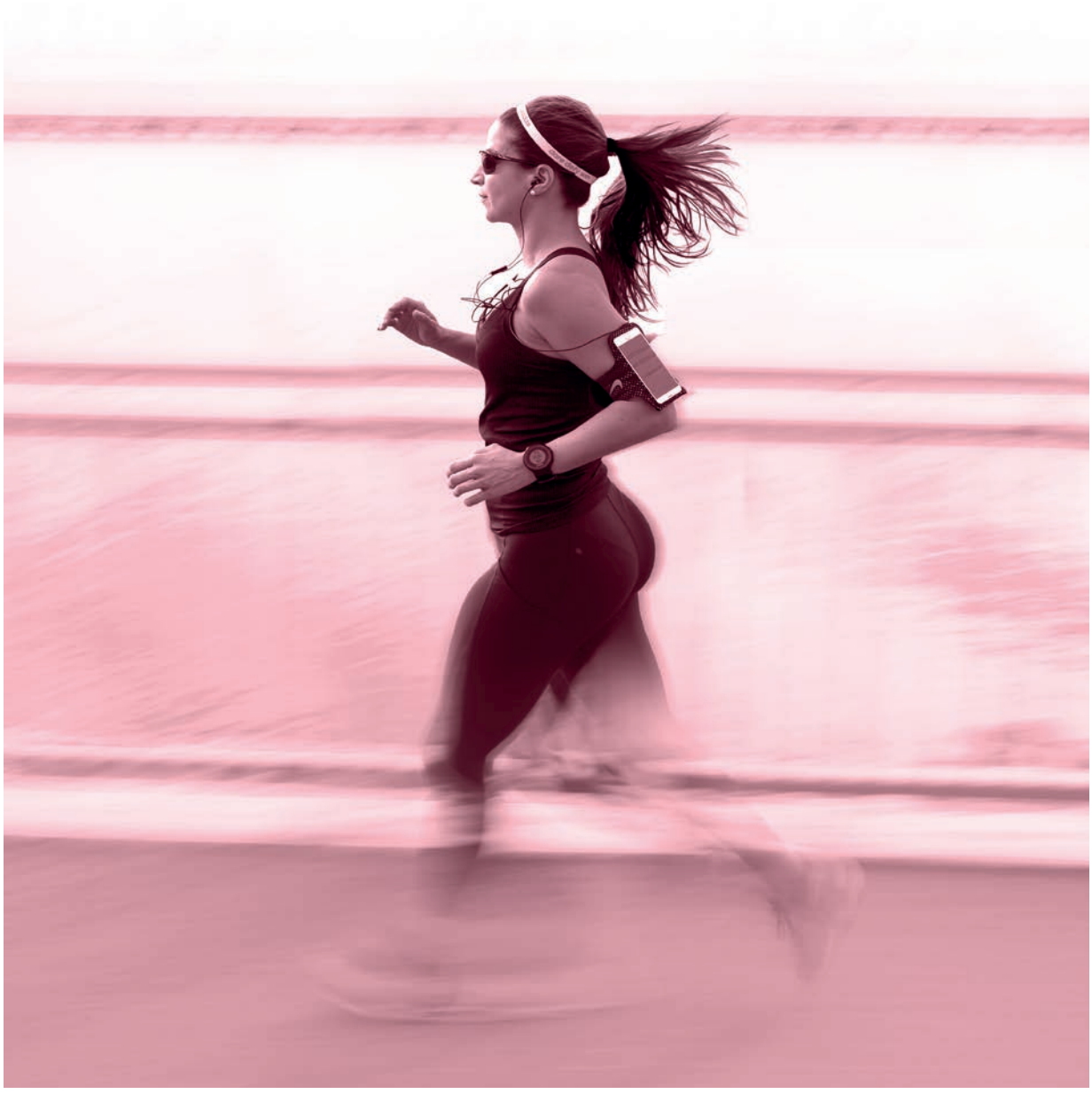
Det skulle behöva bli tydligt vilken prövning som sker via Etikprövningsmyndigheten och vilket ansvar de tar för att kontrollera en forskares beskrivning utifrån kraven i dataskyddsförordningen.

NIS-direktivet

I Sverige genomförs NIS-direktivet genom en ny lag, *Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.* NIS-direktivet är ett direktiv om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen.

Leverantörer av samhällsviktiga tjänster som finns inom sektorerna energi, transport, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, leverans och distribution av dricksvatten samt digital infrastruktur och som kan vara statliga myndigheter, kommuner, landsting eller företag ska identifieras. Med digitala tjänster avses internetbaserade marknadsplatser, internetbaserade sökmotorer och molntjänster.

I korthet ställs krav på att samhällsviktiga tjänster ska arbeta systematiskt och riskbaserat med informationssäkerhet. Både leverantörer av samhällsviktiga tjänster och digitala tjänster ska rapportera incidenter till Myndigheten för samhällsskydd och beredskap, MSB.



Molntjänster

Molntjänster tillhandahålls ofta av internationella företag. Information som hanteras i ”molnet” kan i praktiken hanteras i många olika länder. Molnleverantören kan lyda under andra länders lagstiftning och tvingas överlämna sina kunders information till myndigheter där. Den som använder en molntjänst för sin personuppgiftsbehandling är personuppgiftsansvarig för behandlingen även om den utförs av molntjänstleverantören eller dess underleverantörer.

Innan en molntjänst tas i bruk måste den personuppgiftsansvarige bedöma om den personuppgiftsbehandling som man vill låta molntjänstleverantören utföra kommer att vara tillåten enligt dataskyddsförordningen. En risk- och sårbarhetsanalys bör genomföras för att bedöma om det är möjligt att anlita molntjänstleverantören för behandling av de tänkta personuppgifterna. Ju större integritetsrisker en viss personuppgiftsbehandling innebär desto högre är kraven på säkerhetsåtgärder. Personuppgiftsansvarig måste också ta ställning till om det finns risk för att personuppgifter kan komma att behandlas för andra ändamål än de ursprungliga.

Om uppgifter som omfattas av sekretess ska behandlas via en molntjänst så är en grundläggande förutsättning att regelverket om sekretess har beaktats. I detta sammanhang är det av intresse att det i dataskyddsförordningen ställs krav på att personuppgiftsbiträdets personal ska omfattas av sekretess och att detta ska regleras via biträdesavtalet. Men enligt Justitieombudsmannens (JO) beslut dnr 3032-2011 är dessa ”alternativa” tystnadsplikter inte alltid tillräckliga för att anse att ett utlämnande kan ske utan att det innebär men (skada) för den som skyddas av sekretessen.

JO:s slutsats, utifrån de specifika förutsättningarna i det aktuella ärendet, blev att varken den avtalsreglerade tystnadsplikten som gäller för biträdets personal eller den form av tystnadsplikt som följde av regleringen i dåvarande personuppgiftslag medförde att det kunde anses stå klart att patientuppgifter kunde lämnas ut till biträdets personal utan att den enskilde eller någon närstående till denne led men.

JO:s bedömning hade i det aktuella fallet kunnat bli annorlunda om personuppgiftsbiträdets personal istället omfattats av ett straffrättsligt ansvar.

JO:s beslut kan ses som ett generellt hinder för myndigheter att använda molntjänster. Molntjänster bygger dock typiskt sett inte på att anställda hos molntjänstleverantören tar del av kundernas uppgifter på det sätt som ärendet avser (personer lyssnar i ärendet av läkardiktat som skrivs ned som en journalanteckning).

Även om det finns anställda hos leverantören som rent tekniskt kan komma åt uppgifterna finns det ofta instruktioner och tekniska åtgärder som begränsar denna åtkomst. Skillnaderna i detta hänseende kan påverka menbedömningen. Till exempel skulle menbedömningen kunna påverkas om en personuppgiftsansvarig krypterat all information i molntjänsten och själv hanterar nycklarna. En rättslig bedömning måste baseras på en viss tjänsts konkreta utformning, inte dess beteckning som molntjänst.

Det är också relevant vilka typer av sekretessbelagda uppgifter som kommer att omfattas av utlämnandet. Möjligheterna att lämna ut uppgifter som omfattas av en sekretessbestämmelse som har så kallad *rakt skaderekvisit* är till exempel större än uppgifter som omfattas av ett så kallat *omvänt skaderekvisit*, exempelvis inom hälso- och sjukvården.

Sammanställning av rapporter och initiativ

Det har genomförts och pågår flera initiativ för att nyttja hälsoinformation på ett bättre och effektivare sätt.

Kvalitetsregister och beslutsstöd

I rapporten *Kvalitetsregister och beslutsstöd – Två sidor av samma mynt* lyfts fram att en framgångsfaktor är ett beslutsstöd som riktar sig både till patienter och hälso- och sjukvårdspersonal för att stärka patientens ställning. I rapporten framgår också att fristående beslutsstöd oftare är effektivare än integrerade beslutsstöd som finns i journalsystem eller läkemedelsförskrivningssystem.

Kvalitetsregister och beslutsstöd beskrivs som två sidor av samma mynt då båda syftar till bättre hälsa genom bättre vård. Kvalitetsregistren möjliggör en utvärdering av vårdkvaliteten och underlättar ett systematiskt förbättringsarbete. För att understödja detta är det viktigt att statistik tas fram och analyseras samtidigt som forskning bedrivs.

Kvalitetsregister samlar in information som möjliggör en retrospektiv utvärdering av vårdkvaliteten. Beslutsstöd använder och bearbetar information om patients hälsotillstånd och behandling i kombination med medicinsk kunskap för att generera patientspecifika rekommendationer som prospektivt kan främja vårdkvaliteten. I och med att syftena med beslutsstöd och kvalitetsregister skiljer sig åt faller de under olika legala regelverk. Beslutsstöd omfattas till exempel av kraven på CE-märkning då de utgör medicintekniska produkter eftersom de har ett medicinskt syfte. Syftet med kvalitetsregister är inte att individdata ska användas för vård. Det finns dock system som både innehåller en beslutsstödsdel och kvalitetsregister. I rapporten *Kvalitetsregister och beslutsstöd – Två sidor av samma mynt* framgår det att för att skapa kunskapsgenererade system krävs inte bara kvalitetsregisterdata utan även uppgifter ifrån journalsystem, biobanker och patienten själv. Dessa typer av system är en utvecklingspotential för framtiden.

Laglighetsprövning av realtidsregister inom cancervården

I rapporten *Laglighetsprövning av realtidsregister inom cancervården* tydliggörs att det inte är tillåtet att använda ett nationellt eller regionalt kvalitetsregister för att ge vård i ett enskilt fall, vilket även Datainspektionen påpekat i ett tillsynsbeslut. I tillsynsbeslutet förtydligades också att det är inte är tillåtet att ”tanka hem” uppgifterna i ett kvalitetsregister för att använda dem för beslut om enskilda vårdåtgärder.

Personuppgifter som samlats in i ett kvalitetsregister får inte behandlas för något annat ändamål än kvalitetsuppföljning, statistik och forskning. Det finns dock inget legalt hinder för att till ett kvalitetsregister införa ett beslutsstöd parallellt. Olika vårdgivare (organisationer) kan ha åtkomst till varandras dokumentation om en patient utifrån syftet vård och behandling eller utfärdande av intyg, dock inte kvalitetssäkring (så kallad sammanhållen journalföring). Åtkomst mellan vårdgivare kräver dock som huvudregel ett nödläge eller ett samtycke ifrån aktuell patient.

Framtidens kvalitetsregister

I rapporten *Framtidens kvalitetsregister* framgår att flera utvärderingar visar att mycket har utvecklats positivt men att det finns stora utmaningar i att registren ska användas mer till att förbättra vården och komma närmare den dagliga vården. Arbetet med registren måste förenklas och tekniklösningarna effektiviseras. En viktig del i detta är anpassning till de stora skiften som planeras i nya dokumentationssystem. Patienterna behöver involveras aktivare i mätning och uppföljning.

EU-förslag

Under våren 2018 kom även ett förslag från Europeiska kommissionen[8] med ett förslag till parlamentet om att revidera PSI-direktivet (*Directive on the re-use of public sector information*) som säkerställer tillgång till och vidareutnyttjande av data från den offentliga sektorn. Kommissionens mål med förslaget är att uppnå den fulla potentialen av digital teknik för att förbättra hälsovården och den medicinska forskningen. En del av förslaget går ut på att öka tillgången till offentligt finansierade forskningsresultat men även att offentliga företag ska omfattas av kraven i direktivet och inte bara offentliga myndigheter. PSI-direktivet har införlivats i Sverige via *lagen om vidareutnyttjande av handlingar från den offentliga förvaltningen*, den så kallade PSI-lagen.

Ytterligare initiativ

Utöver ovanstående pågår flera initiativ inom Europa för att få till ett bättre utnyttjande av hälsoinformation och tillskapande av uppförandekoder utifrån dataskyddsförordningen. Datainspektionen har dock gått ut med en rekommendation att avvakta framtagande av utkast på uppförandekod tills artikel 29-gruppen fått en vägledning på plats.[9]

Ett initiativ i Sverige för att få till en mer ändamålsenlig lagstiftning är Arbetsgruppen Regelverk som Henrik Moberg håller samman. Denna gruppering tittar på rättsliga hinder och legala aspekter för att värna om individens integritet och främja den digitala utvecklingen. [10] Mycket frågeställningar och utvecklingsområden lyftes redan i utredningen R*ätt information på rätt plats i rätt tid*[11] men en stor del av de problemområden som utredningen pekade på kvarstår fortfarande.

8 http://europa.eu/rapid/press-release_IP-18-3364_sv.htm

9 https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/uppforandekoder-och-certifieringar/

10 https://ehalsa2025.se/gemensam-organisation-samverkan/arbetsgrupp-for-regelverk/

11 https://www.regeringen.se/contentassets/909ca5e5ee2a48609b25824e228d6486/ratt-information-pa-ratt-plats-i-ratt-tid-sou-201423-bilaga-4

Ett exempel

För att åskådliggöra problematiken och dagens något komplexa lagstiftning har ett exempel använts.

Exemplet består av ett landsting som upphandlat en privat utförare där verksamheten som landstinget och den privata utföraren bedriver samarbetar med en kommun. Samarbetet rör äldre som är aktuella både inom hälso- och sjukvården hos landstinget och den privata utföraren, men även hos kommunen som ansvarar för stödinsatser utifrån socialtjänstlagen.

De olika aktörerna vill nu förbättra processen mellan de olika aktörerna. För att få hjälp att analysera informationsflödet och processerna mellan de olika aktörerna bedöms att det enbart är ett företag i Indien som kan hjälpa aktörerna, eftersom just det företaget har en produkt och tjänst som nyttjar AI för att analysera en stor mängd data för att effektivisera och förbättra processer. För att kunna hjälpa aktörerna behöver dock det aktuella företaget tillgång till en stor mängd data. Företaget önskar också att få använda informationen för att vidareutveckla sin egen produkt.

Ovanstående innebär en stor del utmaningar för att landstinget, den privata utföraren och kommunen ska kunna förbättra sin verksamhet på det sätt de önskar. Dels uppstår frågan hur de tre verksamheterna kan överföra information mellan de olika organisationerna i syftet kvalitetssäkring. Att tillfråga samtliga äldre om samtycke anses inte vara en framkomlig väg.

Det kan också ifrågasättas vilken rätt de olika aktörerna har att behandla varandras personuppgifter för detta syfte samt att samla in den stora mängd data som krävs för att genomföra analysarbetet.

Nästa problem blir att de vill använda ett personuppgiftsbiträde som ska behandla och samköra uppgifterna från de olika aktörerna och som befinner sig i ett tredje land utan adekvat skyddsnivå. Att företag önskar använda aktörers data för att vidareutveckla produkter som bygger på AI är inte ovanligt men ställer till problem då detta som huvudregel inte är tillåtet.

KONKRET INNEBÄR DETTA UTMANINGAR MED:

- Sekretessgränser mellan vårdgivare
- Regelverket för kvalitetsuppföljning
- Rätten att behandla personuppgifter
- Överföring till tredje land
- Molntjänstlösningar
- Uppgiftsminimerings- och lagringsminimeringsprincipen
- Utlämnande av uppgifter som omfattas av sekretess till ett personuppgiftsbiträde

Förslag på angreppsätt

För att uppnå en eventuell plattformslösning för att möjliggöra patientcentrerad datahantering finns det legala möjligheter redan nu, men de är komplexa och medför inte riktigt en smidig tillgång till data och patientuppgifter.

Under rubrikerna *Flera personuppgiftsansvariga* och *Gemensamt personuppgiftsansvar* anges vilka legala möjligheter som finns i dag. Under rubriken *Framtidsdiskussion – En personuppgiftsansvarig* redogörs för ett tillvägagångssätt som i dag inte har stöd i lag, men liksom de andra förslagen i framtidsdiskussionsrutorna är det till för att väcka diskussion och tankar.

Blockchain och uppförandekoder har också samlats i separata rubriker under förslag på angreppssätt. De kan inte ensamma lösa frågeställningen men de är tillvägagångssätt och tekniker som på sikt kan stötta för att uppnå den funktionalitet som efterfrågas av nya plattformslösningar.

Flera personuppgiftsansvariga

Vilket framgår i avsnitt *Sammanställning av rapporter och initiativ* så är det inte tillåtet att ett kvalitetsregister bidrar till ett beslutsstöd. Däremot är det motsatta tillåtet och börjar ske i allt större utsträckning för att undvika dubbelregistreringar och onödigt administrativt arbete.

Utifrån nuvarande lagstiftning kan man tänka sig en plattform som flera olika vårdgivare nyttjar men där patientuppgifterna är logiskt åtskilda. Vårdgivarna kan då via denna plattform dokumentera patientuppgifter som behövs för att ge en god och säker vård. Uppgifter som ska överföras till ett eller flera kvalitetsregister kan överföras via plattformslösningen – antingen till ett kvalitetsregister inom lösningen eller i en annan digital lösning. Vårdgivarna skulle kunna ta del av varandras patientuppgifter för syftet vård och behandling utifrån regelverket rörande sammanhållen journalföring.

Vårdgivarna skulle också själva kunna lämna ut uppgifter för forskning under förutsättning att utlämnande kan ske utifrån regelverket i offentlighets- och sekretesslagen, eller så skulle vårdgivarna kunna ge tydliga instruktioner till ett eventuellt personuppgiftsbiträde hur uppgifter får lämnas ut för forskning. (Ett personuppgiftsbiträde är någon som behandlar personuppgifter på uppdrag av en personuppgiftsansvarig till exempel en vårdgivare.)

För att få till en smidig utlämnandeprocess skulle det skulle underlätta om landets, framförallt, offentliga vårdgivare hade samsyn gällande vad som anses vara anonymiserat respektive pseudonymiserat samt att sekretessprövningen kunde automatiseras mer än vad som sker idag.

Patienter skulle också själva via plattformen, under vissa förutsättningar, kunna bidra till ett kvalitetsregister eller vårddokumentation under förutsättning att det finns tydliga instruktioner vad vårdgivaren önskar för information av patienten. Det kan också tänkas att en del av plattformen är patientens ”egen” som patienten själv helt förfogar över, likt *Hälsa för mig*.

Hälsokontot *Hälsa för mig* är tänkt att vara en lagringsplats för den enskildes samlade hälsouppgifter.[12] Den juridiska grunden att ha en sådan lösning har dock diskuterats och Datainspektionen har haft synpunkter på just *Hälsa för mig*[13] och detta har prövats i Förvaltningsrätten. Problemet är dels vem som är personuppgiftsansvarig för det patienten registrerar, dels vilket rättsligt stöd den personuppgiftsansvariga har att faktiskt behandla dessa uppgifter.

Trots det tillsynsbeslut som *Hälsa för mig* drabbades av, så råder inga tvivel om att en plattform med samlade hälso- och sjukvårdsuppgifter om en person skulle kunna vara till stor nytta genom att informationen automatiserat kan analyseras och trender tidigt fångas upp. Det gynnar individen. Hälso- och sjukvårdspersonalen skulle i ett system – där en stor mängd data automatiskt analyseras utifrån vissa förutbestämda kriterier – effektivare kunna hitta trender och områden där stöd eller vård behöver sättas in, utan att hälso- och sjukvårdspersonalen själv läser all den data som samlats in.

Ovanstående scenario är legalt möjligt men det tillåter inte att kvalitetsregisterinformationen används för vård och behandling. Inte heller får uppgifterna tankas över från kvalitetsregistret (åtminstone inte utan patientens samtycke) till vårdgivarna för syftet vård och behandling. Forskare som önskar ta del av patientuppgifterna behöver begära ut dem från respektive vårdgivare. Det innebär att det går åt många förfrågningar för att få tillgång till samtliga uppgifter på plattformen. Om samtliga vårdgivare och andra personuppgiftsansvariga som har uppgifter

12 https://www.halsaformig.se

13 https://www.datainspektionen.se/globalassets/dokument/beslut/2017-04-25-halsa-for-mig.pdf

på plattformen gett tydliga instruktioner till personuppgiftsbiträdet som driftar plattformen om utlämnande, finns det möjlighet att denna process kan förenklas något. Utlämnandet måste dock alltid ha stöd i gällande sekretessregler.

Gemensamt personuppgiftsansvar

En annan möjlighet som finns är ett gemensamt personuppgiftsansvar. Det innebär att det är två eller flera som gemensamt bestämmer över en viss behandling och att de är personuppgiftsansvariga tillsammans. Då måste de sinsemellan bestämma vem som är ansvarig för att fullgöra de olika skyldigheterna i dataskyddsförordningen. Exempelvis kan en av de personuppgiftsansvariga, som är gemensamt personuppgiftsansvariga, ta på sig ansvar för att teckna biträdesavtal med eventuella personuppgiftsbiträden. Det skulle kunna innebära att antalet avtal blir lägre än om varje personuppgiftsansvarig skulle behöva teckna dessa var och en för sig.

Administrationen kan alltså minska vid ett gemensamt personuppgiftsansvar, då de som är gemensamt personuppgiftsansvariga kan fördela skyldigheterna utifrån dataskyddsförordningen mellan sig.

Uppförandekoder

Uppförandekoder kan tas fram av sammanslutningar och organ som företräder kategorier av personuppgiftsansvariga (eller personuppgiftsbiträden) och är till för att specificera dataskyddsförordningen. Utkastet på uppförandekod ska godkännas av Datainspektionen. Datainspektionen rekommenderar i dagsläget att man ska invänta att ta fram en uppförandekod tills den EU-gemensamma vägledningen om uppförandekod finns på plats.

En framkomlig väg är att föra diskussioner med Sveriges Kommuner och Landsting (SKL) och Inera – samt eventuellt fler organ/sammanslutningar som företräder de personuppgiftsansvariga – för att efterhöra hur de tänker kring uppförandekod och om det finns något arbete för att ta fram detta och i så fall för vilka delar i dataskyddsförordningen. Detta skulle underlätta harmoniseringen inom området.

Uppförandekod omfattar dock bara dataskyddsförordningen; regelverket utifrån till exempel patientdatalagen eller lag om etikprövning och så vidare omfattas inte av detta, så det löser inte ut alla de juridiska förutsättningarna som beskrivits i denna analys.

Blockchain

Blockchain, eller *blockkedja* som det heter på svenska, är enkelt uttryckt en distribuerad databas som lagrar transaktionsinformation i så kallade block, vilka sedan länkas samman i en kedja. En distribuerad databas är en databas där alla deltagare i nätverket har tillgång till databasen på samma villkor. Det finns med andra ord inte någon central aktör som kontrollerar informationen i databasen.

När ett nytt block adderas till blockkedjan verifieras informationen via en matematiskt beräknad digital signatur, även kallad hash. Denna beräkning utgår alltid från det senaste blocket i kedjan och genom denna metod säkerställs att informationen i blockkedjan inte ändras eller manipuleras. Eftersom signaturinformationen är öppen för alla deltagare i nätverket, kan alla deltagare också kan kontrollera riktigheten i informationen. Om någon i efterhand försöker ändra informationen i ett block, kommer den digitala signaturen också att ändras, vilket kommer resultera i att kedjan bryts.

BLOCKCHAIN, GDPR OCH HÄLSO- OCH SJUKVÅRDEN

Blockchain-tekniken[14] innebär både möjligheter och utmaningar sett ur ett GDPR-perspektiv. Många tittar just nu på möjligheterna med att använda blockchain-teknik i syfte att skapa transparenta och säkra databaser, där det samtidigt är möjligt att säkerställa identiteten av deltagare i nätverket och legitimiteten i informationen i

14 http://www.blockchainbloggen.se/halso-sjukvard/

FRAMTIDSDISKUSSION

EN PERSONUPPGIFTSANSVARIG

Det finns idag inte en och samma organisation som har till uppdrag att lagra heltäckande vårdinformation från landets samtliga vårdgivare för att tillhandahålla denna information för syftet vård och behandling, kvalitetssäkring och forskning. Flera olika myndigheter har uppdrag att som personuppgiftsansvariga samla in och/eller behandla delar av den information som vårdgivare skapar och för vissa specifika syftet. Exempel på detta är Socialstyrelsens hälsodataregister och eHälsomyndighetens läkemedelsförteckning. Dessa register är dock inte heltäckande för alla vårduppgifter och får heller inte behandlas för alla de syften som plattformen efterfrågar.

En förändrad lagstiftning där en myndighet får i uppgift att samla in och behandla en större mängd vårdinformation ifrån vårdgivare och uppgifter ifrån patienter, för flera olika syften såsom vård och behandling, forskning och kvalitetsuppföljning skulle underlätta nyttjande av den värdefulla information som redan finns spridd i flera olika system och register. Det skulle dock också kunna innebära stora integritetsrisker. Detta är dock inget som finns legalt stöd för i dagens lagstiftning.

systemet. Blockchain-tekniken går till exempel att använda för att generera så kallade smarta kontrakt. Ett *smart kontrakt* är en automatiserad process och kan fungera som ersättare eller komplement till exempelvis juridiska kontrakt, logistiska transaktioner eller identitetshantering. Inom hälso- och sjukvård skulle ett smart kontrakt till exempel kunna användas för att inhämta samtycke från patienter för behandling av personuppgifter i specifika fall, såsom vid delning av vårduppgifter. Andra möjligheter inom hälso- och sjukvårdsområdet anses till exempel vara att sjukhus, apotek, vårdcentraler med flera ska kunna gå ihop och bilda en blockkedja för att lagra medicinska data, vilken drivs av ett distribuerat nätverk av datorer. På så sätt skulle man kunna samla data från alla olika aktörer inom hälso- och sjukvård i en stor databas. På så sätt skulle dessa aktörer snabbt och enkelt kunna dela med sig av data.

Det problematiska med Blockchain-tekniken ur ett GDPR-perspektiv är att den bygger på att informationen är öppen och oföränderlig, medan GDPR ställer krav på konfidentialitet och radering av personuppgifter i vissa fall. De som utvecklar nya system baserade på Blockchain-teknik måste därför först och främst säkerställa att personuppgifter inte obehörigen röjs genom den information som är publik i blockkedjan. En lösning som utvecklare just nu tittar mycket på är att utesluta faktiska personuppgifter i blockkedjan och istället använda sig av krypterad information i själva kedjan.

I och med att det inte är möjliga att radera uppgifter i en blockkedja, bör samtycke inte användas som rättslig grund för behandling av personuppgifter i en blockkedja. Samtycke innebär att flera rättigheter aktualiseras, som rätten att få sina personuppgifter raderade/rätten att bli glömd. Behandling av personuppgifter på den grunden är alltså sannolikt inte framkomlig för blockkedjan om inte någon teknisk lösning för att säkerställa att personuppgifterna blir anonymiserade i blockkedjan tas fram.

Myndigheter ska dock som utgångspunkt inte använda sig av samtycke som rättslig grund för personuppgiftsbehandlingar som de är ansvariga för. Oftast är det den rättsliga grunden ”uppgift i allmänt intresse eller led i myndighetsutövning” som blir aktuell. Det betyder att en myndighet endast är skyldig att radera personuppgifterna i de fall en registrerad har invänt mot behandlingen och det saknas berättigade skäl för behandlingen. Alltså måste även en myndighet beakta att personuppgifter eventuellt kan komma att behöva raderas, även om detta torde vara ovanligt förekommande.

FRAMTIDSDISKUSSION

OM FRAMTIDSDISKUSSIONERNA

Under rubrikerna *Framtidsdiskussion* har idéer och tankar löpande lyfts kring hur tillgången till patientuppgifter och data skulle kunna underlättas om lagstiftningen ändrades från dagens reglering. Det har dock inte koppling till pågående lagstiftningsarbete utan är till för att väcka diskussion och tankar. Här nedan återfinns en sammanfattning av samtliga diskussionspunkter i dokumentet:

- Generella samtycken och ett nationellt samtyckesregister (opt out)
- Dataportabilitet som krav för samtliga lagliga grunder och alla personuppgifter
- Uppgiftsminimeringsprincipen och lagringsminimeringsprincipen
- Begränsningen i patientdatalagen om vilka patientuppgifter som får samlas in och dokumenteras
- En personuppgiftsansvarig med möjlighet att samla in och behandla personuppgifter för flera olika syften och från ett stort antal vårdgivare
- Gränsdragningen mellan de etiska frågeställningarna i etikprövningen och ställningstagandet om integritetsskyddet via dataskyddsförordningen
- Gemensam nationell syn på anonymisering och pseudonymisering. Automatgenererad sekretessprövning

UNDERLAG OCH RAPPORTER SOM LEGAT TILL GRUND FÖR ANALYSARBETET

- Laglighetsprövning av realtidsregister inom cancervården (Manolis Nymark)
- Aktuella rättsfrågor och lagstiftningsarbeten 2017 (Manolis Nymark)
- Personuppgiftsansvaret och GDPR (Manolis Nymark)
- Kvalitetsregister och beslutsstöd – Två sidor av samma mynt (QRC Stockholm)
- Swelife Forskningsplattformen (Swelife)
- Förslag: Framtidens Kvalitetsregister (SKL)
- Sammanfattning av satsningen 2012–2016 på Nationella Kvalitetsregister (SKL)

Projektet

Rapporten är ett resultat av det delprojekt i SWEPER som handlar om juridik. Mer om SWEPER hittar du på swelife.se. Där hittar du också mer information om det det partnerskap som stöttar SWEPER och flera av de nämnda rapporterna.

DELTAGANDE AKTÖRER I DELPROJEKTET:

- AstraZeneca
- Chorus AB
- LIF
- Regionalt cancercentrum Syd
- Regionalt cancercentrum Uppsala Örebro
- Region Skåne
- Roche
- Stockholms Läns Landsting
- Swedish Medtech
- Västra Götalandsregionen

RAPPORTEN

Rapporten skrevs av Moa Malviker Wellermark på Secure State Cyber på uppdrag av SWEPER-projektet.

Bilder av Andres Urena, Filip Mroz, Rawpizel via Unsplash; alla bilder Creative Commons.

KONTAKTPERSON OCH DELPROJEKTLEDARE

Fred Kjellson
Innovationsledare Innovation Skåne
Telefon: +46 766 48 60 76
E-post: fred.kjellson@innovationskane.com

KONTAKTPERSON SWEPER

Lars Lindsköld
Portföljägare Swelife
Telefon: +46 705 40 65 20
E-post: lars.lindskold@swelife.se

DETTA ÄR SWELIFE

Swelife stödjer samverkan mellan akademi, näringsliv och hälso- och sjukvård med målet att stärka life science i Sverige och förbättra folkhälsan.

Det är ett strategiskt innovationsprogram som finansieras av regeringen via innovationsmyndigheten Vinnova och av programmets deltagande parter.

Swelife är en möjliggörare. Genom ett långsiktigt och nationellt perspektiv ska arbetet bidra till att:

- Life science-sektorns kompetenser och resurser används nationellt genom samverkan och samordning
- Sverige erbjuder goda förutsättningar för en hållbar tillväxt och internationell konkurrenskraft för life science-sektorn
- Invånare i Sverige har tillgång till innovativ, jämlik och individanpassad behandling.

KONTAKT

Peter Nordström
Programchef
peter.nordstrom@swelife.se
+46 705-191 220

info@swelife.se
Besöksadress: Lunds universitet, MNO-huset, Sölvegatan 16, 223 62 Lund
Postadress: Lunds universitet, Swelife, Box 117, 221 00 Lund

Med stöd från
VINNOVA
Energimyndigheten
FORMAS
Strategiska innovations-program

INNOVATION SKÅNE SWElife