Koncernkontoret		
Koncernstab kansli informationssakerhet@skane.se	**Datum**: 2018-05-07 Dnr:	
Dokumentförvaltare: Dataskyddsombudet Koncernkontoret		**Dokumentets status**: Fastställt
Dokumentid: Personuppgiftsbehandling i Region Skåne - Sammanställning av regler och krav **Dokumentformat:** A4	**Version:** 3.0	**Dokumenttyp:** Instruktion **Dokumentklass:** Styrande dokument **Ämne:** Ledningssystem för informationssäkerhet

Personuppgiftsbehandling i Region Skåne - Sammanställning av regler och krav

Revisionshistorik

Datum	Ver.	Namn	Kommentar
2012-10-11	1.0	Enheten för informationssäkerhet	Ersätter tidigare ”Anvisningar för behandling av personuppgifter i Region Skåne – PM” (2008 rev 2010)
2016-07-18	2.0	Personuppgiftsombudet	Uppdaterat dokumentet, tagit bort obsoleta delar.
2018-05-07	3.0	Personuppgiftsombudet	Uppdaterat dokument inför EU:s dataskyddsförordning

Inledning

Inom Region Skåne hanteras stora mängder information, som i stor utsträckning består av personuppgifter. Dessa utgör till stor del underlag för vård och behandling och hanteras i hög grad med IT-stöd. Medborgare/patienter och medarbetare måste ha tillit och förtroende för att informationen är tillgänglig för *behöriga*, att den är skyddad från *obehöriga* och att den är *riktig* och *oförvanskad*.

Denna sammanställning har tagits fram som ett hjälpmedel för vad som ska iakttas vid behandling av personuppgifter. Sammanställningen gäller för såväl intern som extern behandling av personuppgifter som Region Skåne ansvarar för vare sig behandlingen utförs av medarbetare eller IT-tjänsteleverantörer. Sammanställningen gäller också omvänt när Region Skåne behandlar personuppgifter för annan organisations räkning. Behandling av patientrelaterade personuppgifter liksom kommunikation med sådana uppgifter över öppna nätverk kräver särskild uppmärksamhet då informationen omfattas av sekretess och är mycket integritetskänslig.

Regler och krav i denna sammanställning är generellt utformade. I de fall regionspecifika riktlinjer/anvisningar gäller, hänvisas till rutiner i Region Skånes ledningssystem för informationssäkerhet på www.skane.se/informationssakerhet. Ledningssystemet uppdateras fortlöpande.

Under avsnitten Legala krav och Säkerhetskrav behandlas särskilda definitioner och krav till följd av lagstiftningen.

Legala krav

Patientdatalagen/PDL (SFS 2008:355) och Socialstyrelsens föreskrifter och allmänna råd (HSLF-FS 2016:40) om journalföring och behandling av personuppgifter i hälso- och sjukvården reglerar personuppgiftsbehandling i patientjournal och kvalitetsstudier mm i vården samt nationella och regionala kvalitetsregister. Personuppgiftsbehandling i forskningsstudier eller i andra projekt som inte innehåller patientuppgifter regleras av dataskyddslagstiftningen[1]. Utöver nämnda lagar styrs hälso- och sjukvårdens personuppgiftsbehandling också av *Lagen om hälsodataregister (SFS1998:543)*. För IT-stöd som hanterar patientuppgifter innebär detta att lagstiftningens krav om spärr av patientuppgifter, stark autentisering, logg och loggуppföljning, aktiva val m.m. ska uppfyllas.

Personuppgiftsansvarig/PUA. Region Skåne som organisation är personuppgiftsansvarig för behandling av alla personuppgifter som sker internt och externt för regionens räkning således även då den faktiska hanteringen sker av en extern part, t.ex. en IT-tjänsteleverantör. Den externa parten är då ett s.k. personuppgiftsbiträde (se nedan). Vid upphörande av personuppgiftsbiträdes behandling ska personuppgifterna återbördas till Region Skåne. Det är den personuppgiftsansvariges ansvar att ha en förteckning över alla behandlingar som sker. Om en ny behandling påbörjas, t.ex. ett nytt register förs för ett kvalitetssäkringsprojekt, så måste således en sådan anmälan ske, se nedan under punkten *Anmälan om personuppgiftsbehandling*.

Personuppgiftsbiträde/PUB. IT-tjänsteleverantör eller annan organisation som utför personuppgiftsbehandling för Region Skånes räkning är ett personuppgiftsbiträde. På motsvarande sätt kan Region Skåne vara biträde och behandla personuppgifter för annan organisations räkning. Ett biträde får bara behandla personuppgifter i enlighet med instruktioner

[1] Dataskyddsförordningen (EU) 2016/679 och Dataskyddslagen (2018:218).

från personuppgiftsansvarig. Ett personuppgiftsbiträdesavtal *måste* upprättas alternativt ska klausul härom ingå i huvud-/leverantörsavtal. Det är den personuppgiftsansvariges ansvar att se till att biträdesavtal/klausul upprättas. När avtalstiden upphör ska informationen återbördas till den personuppgiftsansvarige.

Etikprövningsnämnd/EPN. Känsliga personuppgifter, såsom de definieras i dataskyddsförordningen (särskilda kategorier) får behandlas för forskningsändamål om behandlingen har godkänts av EPN. Har EPN godkänt en studie och nämnden har tagit ställning till behandling av känsliga personuppgifter omfattas studien av ett viktigt allmänt intresse i Dataskyddslagens bemärkelse. Efter EPN:s godkännande ska beslut om utlämnande av uppgifterna fattas av biträdande medicinsk direktör efter samråd med KVB, enligt punkten *KVB, Central prövningsinstans för utlämnande av uppgifter för forskning* nedan. Personuppgiftsbehandlingen ska därefter även anmälas till den personuppgiftsansvariges register, se avsnittet *Anmälan om personuppgiftsbehandling* nedan.

Överföring till tredje land. Huvudregeln är att ett förbud gäller mot att föra ut personuppgifter utanför EU eller EES. Inom Region Skåne ska ett särskilt beslut fattas om personuppgifter ska lagras eller behandlas utanför EU eller EES. Beslutet fattas av informationsägaren. Dataskyddsförordningen medger att överföring av personuppgifter som är under behandling eller ska behandlas till ett tredje land endast får ske om EU-kommissionens har beslutat att landet uppfyller dataskyddsförordningens krav på adekvat skyddsnivå eller att EU-kommissionens standardavtalsvillkor används vid avtalsskrivandet med personuppgiftsbiträdet. För överföring av personuppgifter till USA krävs även att personuppgiftsbiträdet är anslutet till Privacy Shield eller att EU-kommissionens standardavtalsvillkor används.

Se mer om detta på Integritetsskyddsmyndighetens webbplats,
https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/overforing-utanfor-euees/

Anmälan om personuppgiftsbehandling. Den som initierar en personuppgiftsbehandling i Region Skåne ansvarar för att den anmäls till förvaltningens DSO-företrädare i det så kallade DSF-registret (register med förteckning över alla personuppgiftsbehandlingar som sker i den personuppgiftansvariges verksamhet). Anmälningsrutiner finns under Anvisningar, instruktioner, rutiner/Hantering av personuppgifter i ledningssystemet på www.skane.se/informationssakerhet och uppgift om vem som är DSO-företrädare på respektive förvaltning finns under *Kontakt* på http://intra.skane.se/informationssakerhet.

Bevarande/gallring. Personuppgiftsansvarig bestämmer vilka rutiner och regler som ska gälla för bevarande/gallring av uppgifter i sina personuppgiftsbehandlingar, se www.skane.se/regionarkivet. Gallring ska utföras på sådant sätt att informationen inte kan återskapas.

Informationsskyldighet/registerutdrag. Personuppgiftsansvarig måste informera registrerade om att personuppgiftsbehandling sker i dess verksamheter. I Region Skåne görs detta antingen genom allmänna broschyrer, anslag och webbinformation eller mer riktat vid forsknings-/kvalitetsstudier, se anvisning för *Personuppgiftsbehandling i forsknings- och kvalitetsstudier* på http://www.skane.se/informationssakerhet. Information ska också lämnas ut efter begäran av den registrerade, s k registerutdrag enligt artikel 15 dataskyddsförordningen. Sådan begäran ska göras skriftligen till den personuppgiftsansvarige, inom Region Skåne sker begäran till journal- och arkivservice eller till dataskyddsombudet.

Skyldigheter gällande registrerades rättigheter.

Registerutdrag: Personuppgiftsansvarig är skyldig att lämna information till den registrerade om alla personuppgifter som behandlas om denne. Personuppgiftsansvarig ska också lämna en kopia av de personuppgifter som behandlas, om den registrerade begär det. Rätten begränsas för det fall uppgifter omfattas av sekretess gentemot den registrerade, om uppgifterna endast förekommer i ostrukturerat arbetsmaterial eller om uppgifterna inte säkert kan identifieras.

Rättelse: Personuppgiftsansvarig är skyldig att på begäran eller självmant rätta uppgifter som är felaktiga (innehåller sakliga fel eller uppgifter som inte får behandlas) och komplettera ofullständiga personuppgifter.

Rätten att bli glömd: Personuppgiftsansvarig är under vissa omständigheter skyldig att radera personuppgifter, exempelvis om personuppgifterna inte längre är nödvändiga för ändamålet med behandlingen eller om den registrerade återkallar sitt samtycke och behandlingens rättsliga grund endast är den registrerades samtycket. Inom offentlig förvaltning är rätten begränsad då undantag finns för möjlighet att till arkivering och bevarande.

Begränsning: Personuppgiftsansvarig är under vissa omständigheter skyldig att begränsa behandlingen av en registrerads personuppgifterna. Med begränsning menas 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. I sådana fall kan den registrerade även begära att behandlingen av uppgifterna begränsas under tiden uppgifternas korrekthet utreds.

Dataportabilitet: Personuppgiftsansvarig är under vissa omständigheter skyldig att kunna överföra den registrerades personuppgifter i ett strukturerat, elektroniskt format till en annan personuppgiftsansvarig, så kallad dataportabilitet. Rättigheten för den registrerade gäller endast om samtycke eller avtal används som rättslig grund för personuppgiftsbehandlingen.

Invädning: Personuppgiftsansvarig är under vissa omständigheter skyldig att hantera invändningar som den registrerade gör mot en pågående behandling av dennes personuppgifter. Rättigheten gäller endast om allmänt intresse, myndighetsutövning eller berättigat intresse används som rättslig grund för personuppgiftsbehandlingen. Rätten att göra invändingar innebär att personuppgifterna inte längre får behandlas om inte den personuppgiftsansvarige kan visa vilken rättslig grund som är tillämplig för behandlingen.

Därutöver finns en skyldighet att efter begäran blockera eller utplåna felaktiga uppgifter. För personuppgifter som omfattas av PDL:s regler finns bestämmelser i PDL om förstöring av journal i samband med IVO:s beslut. Region Skånes rutiner för detta finns i anvisning för *Journalförstöring och rättelse av journal* på http://www.skane.se/informationssakerhet.

Säkerhetskrav

Generellt

Regionstyrelsen har beslutat om Riktlinjer för informationssäkerhet. Riktlinjen fastställer det övergripande ansvaret för informationssäkerhet inkluderande behandling av personuppgifter och skyddet av dem. Vilka konkreta säkerhetsåtgärder som behöver vidtas är ett resultat av dels den konsekvensbedömning som ska göras och som beskrivs kort nedan samt den informationsklassificering och den riskanalys som också ska genomföras.

Kraven är desamma oavsett om Region Skåne som PUA behandlar personuppgifterna eller om behandlingen lagts ut på personuppgiftsbiträde. Avtal i form av personuppgiftsbiträdesavtal och instruktioner ska reglera personuppgiftsbehandlingen.

Riskanalys/Konsekvensbedömning
Om en behandling av personuppgifter sannolikt leder till hög risk för de registrerades fri- och rättigheter ska en konsekvensbedömning göras. Konsekvensbedömning kan även göras för sådana personuppgiftsbehandlingar som medför en lägre risk. En konsekvensbedömning ger förståelse för personuppgiftsbehandlingens konsekvenser och risker och är till hjälp för att avgöra vilka säkerhetsåtgärder som ska vidtas eller vilka tekniska lösningar som ska väljas. Konsekvensbedömningen är inte en engångsföreteelse utan en pågående process som behöver omprövas och uppdateras kontinuerligt. Arbetet med konsekvensbedömning ska påbörjas så fort det är praktiskt möjligt och uppdateras i takt med att behandlingens olika delar fastställs. Konsekvensbedömningen görs lämpligast i samband med riskanalys. Konsekvensbedömningar som regleras i dataskyddsförordningen är i princip samma företeelse som en riskanalys.

En riskanalys ska enligt socialstyrelsens föreskrifter alltid genomföras innan en behandling av personuppgifter som omfattas av PDL om det finns en risk för att personuppgifterna kan hanteras på ett sätt som strider mot lagstiftningen.

Säkerhetskraven som kan bli aktuella rör både organisatoriska och tekniska säkerhetsåtgärder. Nedan beskrivs i kort under olika rubriker vad som kan vara aktuellt.

Personal
Arbetsrutiner och organisation ska utformas så att personberoende undviks. Alla som har tillgång till personuppgifter ska genomgå lämplig utbildning och personalen ska vara informerad om vikten av att följa gällande säkerhetsrutiner. Detta gäller såväl personuppgiftsansvarig som personuppgiftsbiträde och i förekommande fall underleverantörer. Rutiner ska finnas för att säkerställa att extern personal som hanterar Region Skånes personuppgifter är bundna av tystnadspliktsavtal. För rutiner och tystnadspliktsavtal se kapitlet om Styrning av åtkomst på http://www.skane.se/informationssakerhet.

Fysisk säkerhet
Informationstillgångar som används för att behandla personuppgifter ska ha ett tillräckligt bra skydd. Skyddet ska vara anpassat till det värde den har för de verksamheter/processer som använder informationen samt de legala krav som informationen omfattas av. Vilka fysiska skyddsåtgärder som behövs avgörs av vilken typ av informationstillgång och de konsekvenser det kan få om skyddet inte kan upprätthållas.

Identifiering
Personal: I Region Skåne används e-tjänstekort för att identifiera personal som behandlar personuppgifter inom hälso- och sjukvård (patientuppgifter).
Patient: Patient ska enligt Patientdatalagen vara säkert identifierad med antingen personnummer, samordningsnummer (utdelas av Skatteverket) eller reservnummer (utdelas av hälso- och sjukvården). För rutiner i Region Skåne se *Identitetshantering för patient* på http://www.skane.se/informationssakerhet → instruktioner för informationssäkerhet → hantering av patientuppgifter.

Skyddade personuppgifter

För hantering av patienter respektive anställda som erhållit skyddade personuppgifter se anvisning för *Skyddade personuppgifter* på www.skane.se/informationssakerhet → instruktioner för informationssäkerhet → hantering av patientuppgifter.

Behörighetskontroll
Behörighetskontrollsystem ska finnas om krav finns att endast behörighet personal ska ha tillgång till information. Krav på behörighetskontroll och utformningen av den avgörs av den klassificering som gjorts genomförd riskanalys. Rutiner för tilldelning och kontroll av behörigheter ska också finnas. Organisationen ska administrera behörigheter för sina egna användare.

Behandlingshistorik (logg)
För att kunna kontrollera vilka som har haft tillgång till personuppgifterna ska finnas en behandlingshistorik (logg). Logg ska följas upp och skyddas mot otillåtna ändringar samt vara så detaljerad att den kan användas för att utreda om personuppgifter har använts felaktigt eller obehörigt. Enligt PDL gäller att registrering/loggning av händelser ska kunna påvisa vem som har berett sig tillgång till patientuppgifter, vilka patientuppgifter som har behandlats, vad behandlingen bestått av och när behandlingen har påbörjats och avslutats samt vid vilken vårdenhet behandlingen skett.

I ett IT-stöd som innehåller patientuppgifter ska logg sparas i minst fem år.

Kommunikation
När personuppgifter överförs via öppna nätverk ska de skyddas mot förstöring, förändring och obehörig åtkomst. Kommunikation ska ske insynsskyddat med någon form av krypteringsstandard. Användare och/eller IT-tjänst hos PUA och IT-tjänst hos PUB ska verifiera varandras identitet med certifikat för att garantera att anslutning sker till avsedd part.

Säkerhetskopiering
För att förhindra förlust av information ska finnas rutiner för säkerhetskopiering samt för återskapande av information. Dokumenterade rutiner ska finnas.

Skydd mot skadliga program
Skyddsåtgärder ska vidtas för att upptäcka och skydda systemet mot skadlig kod.

Reparation och service
Reparation och service ska utföras på ett sådant sätt att personuppgifter inte blir tillgängliga för obehöriga. Anlitas serviceföretag ska avtal först ha tecknats och innehålla bestämmelser om tystnadsplikt samt krav på säkerhetsrutiner som ska tillämpas i samband med servicen. Om service utförs på distans ska servicepersonalen identifieras på ett säkert sätt och endast ha tillgång till utrustningen/personuppgifterna under själva servicetillfället.

Tillgänglighet
Krav på informationens tillgänglighet hos personuppgiftsbiträdet avgörs av den personuppgiftsansvariges verksamhetsbehov och ska vara formulerade i ett tjänstenivåavtal (SLA). Krav på tillgänglighet kan variera mellan olika verksamheter inom Region Skåne och krav på tillgänglighet ska analyseras i samband med informationsklassificeringen.

Rättelse/borttagande av information
Personuppgiftsbiträdet (PUB) ska följa den personuppgiftsansvariges (PUA) direktiv om rättelse/borttagande av information. Rutiner ska finnas hos PUB som behandlar journaluppgifter

att snabbt följa beslut om förstöring från Socialstyrelsen, varvid deadlinedatum för borttag ska beaktas.

Avveckling/förstöring av informationsmedia
Gallringsbart material eller informationsmedium som innehåller personuppgifter och som inte längre ska användas för sitt ändamål ska avvecklas eller förstöras på sådant sätt att uppgifterna inte kan återskapas. Detta gäller oavsett om uppgifterna omfattas av sekretess eller inte. Dokumenterade rutiner ska finnas för denna hantering.

Pseudnymisering
Pseudonymisering är en säkerhetsåtgärd som innebär att personuppgifterna översätts med koder och därmed inte längre är direkt hänförliga till en viss person. Pseudonymisering är en säkerhetsåtgräd som särskilt uppmärksammas i dataskyddsförordningen som ett bra sätt att skydda personuppgifter.

KVB, Central prövningsinstans för utlämnande av uppgifter för forskning

Regionstyrelsen har delegerat till biträdande hälso- och sjukvårdsdirektör att efter samråd med medicinsk, administrativ, informationssäkerhets- och juridisk kompetens fatta beslut i frågor om utlämning av patientuppgifter för forskning. Denna samrådsgrupp kallas för KVB (Kvalitetsregister, vårdinformationssystem och beredning).

Innan forskningsstudier påbörjas, deltagande eller inrättande av i nationellt/regionalt kvalitetsregister planeras, ska anmälan om studien/registret göras till kunskapsstyrning@skane.se. Efter samråd med olika kompetenser i gruppen fattar därefter biträdande medicinsk direktör beslut om tillgång till/utlämnande av patientuppgifter eller inrättande av olika former av register m m kan ske eller inte. Mer detaljer kring denna hantering finns på webbplatsen Vårdgivare Skåne under Forskning i Region Skåne, länk till information KVB.

Termer, begrepp och definitioner

EPN	Regional etikprövningsnämnd som prövar forskningsstudier avseende forskning på såväl levande som avlidna personer, forskning på biologiskt material från människor samt forskning som innebär hantering av känsliga personuppgifter.
HCC	Health Care Certificate. Tjänstecertifikat för de som arbetar inom svensk vård och omsorg och som knyter an till den sjukvårdsorganisation man arbetar i. Se SITHS.
HSA-id	Är en global unik identitet, som byggs upp av beteckning för Sverige, vårdgivarens organisationsnummer och ett unikt löpnummer. Utges till aktörer, tjänster och funktioner inom vård och omsorg. Se SITHS.
Patientuppgift	Patientens personuppgifter dvs uppgifter om patientens hälsotillstånd eller andra personliga förhållande, eller om vidtagna eller planerade vårdåtgärder.
Person-uppgift	All slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet. Inom hälso- och sjukvården är även uppgifter om avlidna att betrakta som personuppgift, enligt Patientdatalagen. Ex: Journalsystem laboratoriemedicinska och patientadministrativa system, kvalitets- och forskningsregister, personaladministrativa system.

PUA	Personuppgiftsansvarig. Är den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter. Är ofta en juridisk person.
PUB	Personuppgiftsbiträde. Den som behandlar personuppgifter för den personuppgiftsansvariges räkning.
DSO	Dataskyddsombud. Är den fysiska person som, efter förordnande av PUA, självständigt ska se till att personuppgifter behandlas på ett korrekt och lagligt sätt.
Registrerad	Den som en personuppgift avser.
SITHS	Säker IT i Hälso- och Sjukvård. Modell som bygger på att anställda inom vård och omsorg har ett personligt elektroniskt ID-kort med ett elektroniskt PKI-certifikat (Public Key Infrastructure). Certifikatet är ett anställningsbevis vilket säkerställer vårdgivarens behörighet. Med kortet kan personen ifråga på ett säkert sätt identifiera sig, t ex i e-post eller mot IT-tjänster av olika slag. SITHS möjliggör säker kommunikation inom och mellan verksamheter.
SLA	Service Level Agreement**.** Avtal mellan kund/PUA och IT-tjänsteleverantör som reglerar servicenivå eller kapacitet (supporttid, svarstider, max driftavbrott)
KVB	Regionstyrelsen har delegerat till biträdande hälso- och sjukvårdsdirektör att efter samråd fatta beslut i frågor om utlämning av patientuppgifter för ändamålet forskning. Denna samrådsgrupp kallas för KVB (Kvalitetsregister, vårdinformationssystem och beredning). I Region Skåne har alltså beslutats att denna samrådsgrupp ska pröva utlämnanden av personuppgifter för forskning, samt inrättande av och deltagande i regionala eller nationella kvalitetsregister