

Regionstyrelsen

Nya riktlinjer för informationssäkerhet och hantering av patientinformation m m i anledning av författningsändringar

Ordförandens förslag

1. Regionstyrelsen fastställer föreliggande förslag till riktlinjer för informationssäkerhet för Region Skåne och upphäver därmed regionstyrelsens tidigare beslut § 66/99.
2. Regionstyrelsen fastställer föreliggande förslag till riktlinjer för tillgång till och utlämnande av patientinformation och upphäver därmed regionstyrelsens tidigare beslut § 69/05 samt hälso- och sjukvårdsnämndens beslut § 8/05 om informationsutbyte mellan externa vårdgivare och Region Skåne.
3. Regionstyrelsen uppdrar åt regiondirektören att fastställa tillämpningsanvisningar för tillgång till och utlämnande av patientinformation och därmed upphäva gällande regler samt fastställa organisation för informationssäkerhetsarbetet.

Beskrivning av ärendet

Patientdatalagen (SFS 2008:355) som trädde i kraft 2008-07-01 ger utökade möjligheter att få direktåtkomst till patientinformation med hjälp av IT-stöd och förutsättning för detta har getts genom ändring i sekretesslagen.

Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården (SOSFS 2008:14) konkretiserar patientdatalagen.

Föreskrifterna uttalar krav på att en policy för informationssäkerhet ska inordnas under ledningssystem för kvalitet och patientsäkerhet samt att ansvariga ska utses för att driva informationssäkerhetsarbetet hos vårdgivaren.

I föreskrifterna poängteras vårdgivarens personuppgiftsansvar. Regionstyrelsen är personuppgiftsansvarig för all personuppgiftsbehandling i Region Skånes verksamheter och beslut föreligger sedan tidigare om att det ska finnas ett personuppgiftsombud i Region Skåne (bil 1).

Tillämpningsanvisningar för journalföring och övrig hantering av patientinformation kommer att utarbetas under 2009 och fastställas av regiondirektören.

Jerker Swanstein
Regionstyrelsens ordförande

Sören Olofsson
Regiondirektör

- Bilaga 1: Beslut om personuppgiftsombud i Region Skåne
- Bilaga 2: Riktlinjer för tillgång till och utlämnande av patientinformation
- Bilaga 3: Informationssäkerhetsriktlinjer
- Bilaga 4: Organisation för informationssäkerhetsarbetet (fastställs av RD)
- Bilaga 5: Tillämpningsanvisningar för tillgång till och utlämnande av patientinformation (fastställs av RD)

Regionkontoret
Kompetenscentrum juridik
Ulf Jakobsson

1998-11-16

Dnr 980197

SKÅNE LÄNS LANDSTING		
Diarlet		
1998 -11- 24	Dok.nr 2	
1000	012	197/98
Personuppgiftsombud enligt Personuppgiftslagen		

Regionstyrelsen

Personuppgiftsombudets formella ställning

Personuppgiftslagen ersätter nuvarande datalag. Den nya lagen är uppbyggd på ett principiellt annat sätt än den tidigare. I överensstämmelse med de grundläggande principerna i EU-rätten läggs stora delar av ansvaret över på användaren, den personuppgiftsansvarige. Så länge denne sköter sig, har han ganska stor frihet inom lagens ramar, men bryter han mot lagens regler drabbas han av hårdare sanktioner än idag. För speciella register kommer man att utfärda särskilda regler. Så har redan skett vad gäller vårdregister. En lag om vårdregister trädde i kraft samtidigt med personuppgiftslagen

Personuppgiftsansvarig är den juridiska personen Region Skåne.

Datainspektionen kommer att finnas kvar, men med ett delvis annat arbetssätt. Det mesta av nuvarande tillståndsgivning försvinner. Dessutom kan delar av det tillsynsansvar Datainspektionen har föras över till den personuppgiftsansvarige, genom att denne utser ett personuppgiftsombud.

Personuppgiftsombudet har givits en slags myndighetsställning, som Datainspektionens förlängda arm. Det är inte nödvändigt att utse ett sådant ombud. Den som inte har ett personuppgiftsombud kommer att få anmäla och i vissa fall begära tillstånd direkt hos datainspektionen. Ansvaret för att behandlingen av personuppgifter sedan sker på ett korrekt sätt och att information lämnas enligt lagens krav åvilar fortfarande den ansvarige. Om dessa uppgifter inte utförs av ett formellt utsett personuppgiftsombud, måste rutiner skapas för att uppgifterna ändå utförs.

Det finns därför anledning att utse personuppgiftsombud för Region Skåne. Ansvaret blir därmed tydligt och man slipper en del byråkrati i form av anmälningar och ansökningar till Datainspektionen.

Det är möjligt att utse flera personuppgiftsombud. T ex kan man ha ett för varje förvaltning eller något annat avgränsat område. Med en sådan organisation uppstår samordningsfrågor och framför allt problem med ansvaret för gemensamma register. Det är därför bättre att utse ett personuppgiftsombud för Region Skåne. Ett ombud för hela regionen har inte möjlighet att ha detaljkunskap om samtliga behandlingar av personuppgifter inom området. En organisation med ett ombud förutsätter att förvaltningarna har tillräckliga resurser för att ansvara dels för informationssäkerheten på det sätt som förutsättes i den antagna policyn dels för en korrekt information till personuppgiftsombudet.

Ombudet måste ges den roll, som lagen förutsätter. Han måste ha en självständig och fristående roll gentemot regionledning och förvaltningar. Man kan därför överväga om det skall vara en anställd som är personuppgiftsombud eller en utomstående, som köps in. En nära anknytning till den egenkontroll, som kvalitetssystemet förutsätter är självklar.

Personuppgiftsombudets uppgifter

Ombudets huvuduppgift är att se till att personuppgifter behandlas på ett korrekt och lagligt sätt. Ombudet skall därför :

- vara informerad om samtliga behandlingar av personuppgifter inom regionen, varvid bör uppmärksammas att behandling av personuppgift är ett mycket vitt begrepp
- svara för att de regler, som styr särskilda behandlingar av personuppgifter, (t ex vårdregisterlagen) följs
- svara för att de informationsskyldigheter, som finns i lagen blir uppfyllda
- svara för att rättelser sker
- svara för att nödvändiga säkerhetsåtgärder vidtages
- återkommande kontrollera användningen av personuppgifter och säkerhetsåtgärder inom regionen, innebärande bl a att han skall ha tillgång till samtliga loggsystem
- svara för att uppgifter om överträdelser påpekas för beslutande organ och – om rättelse ej sker – anmäla till Datainspektionen.
- följa den policy för informationssäkerhet, som gäller vid varje tillfälle

Förslag till beslut

Regionstyrelsen föreslås besluta att för Region Skåne skall utses ett personuppgiftsombud med de uppgifter, som framgår av förslaget.



Stefan Carlsson
Regiondirektör

Riktlinjer för tillgång till och utlämnande av patientinformation

Inledning

Regionstyrelsen antog 2007-06-07 (§ 111) den nationella IT-strategin för vård och omsorg enligt rekommendation från Svenska Kommunförbundets och Landstingsförbundets styrelser. Samtidigt antogs rekommendationen om medverkan i och genomförande av förslaget till handlingsplan för förverkligande av en nationell IT-infrastrukturplattform med början 2007-06-19. Ett insatsområde i strategin - harmonisering av lagar och regelverk med ökad IT-användning - har förverkligats genom patientdatalagens införande halvårsskiftet 2008.

I Vägval Skånegemensamt vårdinformationsstöd antog Regionstyrelsen 2007-06-07 (§ 112) viljeinriktningen att vårdgivare ska ha tillgång till journalinformation över hela Region Skåne.

Tillgång till vårdinformation beslutades 2005 i policy antagen av RS/050129, § 29 samt policy och tillämpning för informationsutbyte mellan externa vårdgivare och Region Skåne antagen av HS/050124, § 8.

Möjligheter och krav

Patientdatalagen ger utökade möjligheter att få elektronisk åtkomst till patientinformation med hjälp av IT-stöd och förutsättning för detta har getts genom ändring i Sekretesslagen. Region Skånes tre tidigare sekretessområden - hälso- och sjukvård, habilitering och hjälpmedel samt tandvård – är numera endast ett sekretessområde.

En förutsättning för att få elektronisk åtkomst är att personal som arbetar hos en vårdgivare ska delta i vården av patienten samt ha behov av uppgifterna för att utföra sitt arbete. Personal kan även av andra skäl behöva uppgifterna för att utföra sitt arbete inom hälso- och sjukvården.

Det ställs också krav på funktioner för att upprätthålla patientintegritet och sekretess i form av behörighetskontroll, spårbarhet med loggning och logguppföljning, som i sin tur ställer krav på säker identifiering av användare. Dessutom möjliggörs för patienten att genom samtycke/spärr påverka vilken information som görs tillgänglig på elektronisk väg. Detta gäller vare sig tillgång ges inom en vårdgivare, s k *inre sekretess* eller tillgången ges mellan vårdgivare, s k *sammanhållen journalföring*.

Lagen ger också möjlighet för vårdgivare att göra viss patientinformation tillgänglig för patienten genom direktåtkomst liksom uppgift om vem som haft åtkomst till dennes information, s k logguppgifter. Patient kan även idag i offentlig sjukvård få tillgång till sin patientinformation liksom logguppgifter men då genom ett formellt utlämnande i enlighet med tryckfrihetsförordningen. Patient kan också få tillgång till sina personuppgifter i vården genom ett registerutdragsförfarande enligt personuppgiftslagen.

Realisering genom överenskomna säkerhetstjänster

Säkerhetslösningar har utvecklats inom ramen för den nationella IT-handlingsplanen för att uppfylla patientdatalagens krav. BIF (bastjänster för informationsförsörjning) möjliggör säker hantering av patientinformation såväl inom sekretessområdet som vid sammanhållen journalföring. I BIF ingår bl a tjänster för åtkomstkontroll med loggning och logganalys, samtycke och utlämnande.

Tillämpning

Region Skåne ska utnyttja de möjligheter patientdatalagen ger för tillgång till patientinformation

- mellan vårdenheter inom det inre sekretessområdet
- mellan Region Skåne och vårdgivare som väljer att ingå i sammanhållen journalföring
- till patient genom direktåtkomst till delar av dennes journalinformation samt logguppgifter.

I tillämpningsanvisningar förtydligas förutsättningar för detta.

Riktlinjer för informationssäkerhet i Region Skåne

Dessa riktlinjer ingår som en del i den övergripande säkerhetspolicyn för Region Skåne och gäller för all informationshantering.

Inom Region Skåne behandlas stora mängder information och personuppgifter, som till stor del utgör underlag för vård och behandling. Medborgare och medarbetare ska kunna känna tillit och förtroende för regionens informationshantering.

Definition

Informationssäkerhet inbegriper all säkerhet kring den totala informationsbehandlingen. Såväl organisatoriska åtgärder som fysiska och logiska skyddsåtgärder inbegrips.

Syfte och Mål

Informationssäkerhetsarbetet i Region Skåne syftar till att informationen ska vara:

- Tillgänglig – behörig användare ska få tillgång till den information som behövs för att utföra sina arbetsuppgifter
- Skyddad – informationen ska vara skyddad mot obehörig åtkomst
- Riktig – informationen ska vara skyddad mot förvanskning eller otillåten förändring
- Spårbar – hantering av information ska kunna följas upp och inte gå att förneka i efterhand

Ansvarsfördelning

Regionstyrelsen har ytterst ansvaret för informationssäkerhet i Region Skåne genom fastställande av dessa riktlinjer.

I Region Skåne ska finnas ansvarig för samordning och utveckling av informationssäkerhetsarbetet.

I Region Skåne ska finnas ett personuppgiftsombud.

Ansvaret för informationssäkerheten följer verksamhetsansvaret. Varje medarbetare har också ett egenansvar.

Genomförande

Informationssäkerhetsarbetet ska bedrivas förebyggande. Arbetet ska inriktas mot att eliminera brister i informationens tillgänglighet, skydd, riktighet och spårbarhet.

Arbetet ska så långt möjligt bedrivas enligt SIS-standard för informationssäkerhet. Region Skånes ledningssystem/Informationssäkerhets-handboken ska vara en integrerad del i den dagliga verksamheten. Riktlinjerna ska följas vid planering, utveckling, ackreditering och upphandling.

Ledningssystemet ska säkerställa att det finns rutiner för risk- och avvikelshantering.

Informationssäkerheten ska upprätthållas genom organiserat arbete med rätt bemanning och kompetens.

Utbildning och information ska genomföras systematiskt och regelbundet. Vägen till säker informationshantering går genom medvetna medarbetare.

Uppföljning

Uppföljning av hur ledningssystemet efterlevs ska ske systematiskt och regelbundet enligt ovanstående ansvarsfördelning.

Informationssäkerhetsansvarig ska minst en gång per år rapportera om händelser och åtgärder av större betydelse till Regionstyrelsen. Rapportering av informationssäkerhetsarbetet ska ingå i verksamheternas årsredovisning.

Författningar och Region Skånes regelverk ska följas. Brister i efterlevnad kan föranleda ett arbetsrättsligt eller straffrättsligt förfarande.

Datum 2009-12-21
 Dnr 0900521

1 (2)



Förslag till organisation för informationssäkerhetsarbetet i Region Skåne

Uppdrag

Uppdrag för avdelning för informationssäkerhet grundas på

- riktlinjer för informationssäkerhet, beslut i RS, 2009-05-12, i vilka kraven på informationssäkerhet från Socialstyrelsens författning 2008:14 innefattas
- uppdrag som personuppgiftsombud för Region Skåne, enligt §§ 38-40 personuppgiftslagen och beslut i regionstyrelsen, 1998-11-24, att utse ett personuppgiftsombud.

Uppdraget omfattar att

- leda, utveckla och följa upp informationssäkerhetsarbetet i regionen
- ansvara för utveckling, införande och revision av Ledningssystem för informationssäkerhet, inkluderande att utarbeta förslag till riktlinjer och anvisningar
- vara personuppgiftsombud Region Skåne med uppgifter enligt PuL § 38-40
- leda grupp med förvaltningarnas samordnare för informationssäkerhetsarbetet
- delta i nationellt arbete/omvärldsbevaka inom området informationssäkerhet

Uppföljning enligt författningarna innebär att

- informationssäkerhetschef ska en gång per år rapportera om händelser och åtgärder av större betydelse till regionstyrelsen
- personuppgiftsombudet ska tillse att uppföljningar görs så att personuppgifter behandlas korrekt enligt Datainspektionens krav.

Nuvarande uppdrag som stf personuppgiftsombud är förenat med operativa uppgifter gentemot medborgare (§ 26-utdrag) och verksamhet (förteckning av register). Utveckling pågår med omfattande digitalisering av dessa uppgifter för utlokalisering till förvaltningarna.

Organisatorisk placering

Avdelning för informationssäkerhet placeras som en avdelning under enheten för juridik inom koncernkontoret med fysisk placering Regionhuset, Lund och kommande placering i Malmö.

Resurser

Behov finns av 3 personer för att utföra uppdraget. 1-informationssäkerhetschef, 1 personuppgiftsombud och 1 person med inriktning mot arbete till följd av konsekvenser av den nya patientdatalagen och Socialstyrelsens föreskrifter 2008:14 härtill. Uppdraget måste dock ses som en helhet för avdelningen Ytterligare en person behöver anställas som stf personuppgiftsombud för att garantera kompetensväxling vid förestående pensionsavgångar. För genomförandet av uppdraget krävs resurser från RSIT med kompetens inom informations-säkerhet, beräknat till 800 tkr - 1 Mkr. Därutöver finns visst behov av medel för anlitanade av externa konsulter för exempelvis uppföljning beräknat till ca 300 tkr.

Samverkan

Samverkan ska ske med samordnare för informationssäkerhet på förvaltningarna, andra säkerhetsfunktioner på regionnivå, med RSIT samt med nationella instanser.

Förslaget föreslås träda ikraft 2010-01-01.

Fastställes 2009-12-21



Karl Gustav Andersson
Tf regiondirektör

Bilaga: Bemanning

Camilla Ziegler
Britt Lagerlund

2009-11-27

Förslag på bemanning av informationssäkerhetsarbetet i Region Skåne

Informationssäkerhetschef, 100 % Fn 30 % uppdrag för Beställarfunktionen vid SKL	Britt Lagerlund
Personuppgiftsombud, 100 %	Eva Plym Forshell
Handläggare med inriktning på PDL-konsekvenser, 100 % Grundanställning som läkare i Primärvården, har under 10 år haft uppdrag inom informationssäkerhet, projektanställning i RSIT-2009-12-31. Arbetar 25 % vid Lunds Universitet	Anders Beckman
Stf personuppgiftsombud, 100 % för kompetensväxling vid pensionsavgångar	Rekryteras kvartal 1, 2010

Tillämpningsanvisningar för tillgång till och utlämnande av patientinformation

Inledning

Hantering av patientinformation inom Region Skåne ska ske utifrån *patientdatalagen* (SFS 2008:355), Socialstyrelsens föreskrift *Informationshantering och journalföring i hälso- och sjukvården* (SOSFS 2008:14) och Region Skånes *Riktlinjer för informationssäkerhet* med anknytande *ledningssystem för informationssäkerhet* (informationssäkerhetshandbok). Dessa tillämpningsanvisningar är gemensamma för all vårdverksamhet inom Region Skåne och gäller all personal som hanterar patientinformation. Patientinformationen ska göras tillgänglig på ett korrekt sätt utifrån verksamhetens behov. Det viktigaste för att tillämpningsanvisningarna ska kunna efterlevas, är att personalen har kunskap och förståelse för dem.

En nationellt överenskommen säkerhetsinfrastruktur har utvecklats för att uppfylla patientdatalagens krav och ska möjliggöra säker hantering av patientinformation. Arbetet med utveckling av tekniska tjänster för detta sker i olika steg och de första tjänsterna beräknas bli levererade under 2009. De tekniska tjänsterna ingår i BIF (bastjänster för informationsförsörjning) och består av autentisering, åtkomstkontroll, vårdrelation, samtycke, utlämnande, kontexthantering, loggning, logganalys, notifiering (meddelande att händelse inträffat) samt administration av regler och egenskaper. Med hjälp av dessa ska Region Skåne kunna tillämpa patientdatalagen.

Dessa tillämpningsanvisningar rör i huvudsak den elektroniska hanteringen av patientinformation. För termer och definitioner se sista sidan.

Grundläggande principer

Inre och yttre sekretess

Region Skånes hälso- och sjukvård inklusive tandvård och habilitering och hjälpmedel utgör ett sekretessområde, där patientdatalagen möjliggör elektronisk åtkomst till patientinformation utan samtycke (inre sekretess). Kravet är dock att personal som arbetar i Region Skåne ska delta i vården av patienten samt ha behov av uppgifterna för att utföra sitt arbete. Personal kan även av andra skäl, t ex ekonomiadministrativa, behöva uppgifterna för att utföra sitt arbete.

Mellan vårdgivare finns yttre sekretess, vilket innebär att patient ska samtycka eller menprövning ske i varje enskilt fall vid informationsutlämnande. Här sker ett formellt utlämnande enligt sekretesslagen.

Det är ansvarsmässigt skillnad mellan inre och yttre sekretess. Vid inre sekretess och vid sammanhållen journalföring blir den befattningshavare som bereder sig tillgång till patientinformationen ansvarig. Vid ett utlämnande av patientinformation till annan vårdgivare åligger ansvaret den befattningshavare som tar ställning till utlämnandet.

Säker identifiering

I Region Skånes vårdverksamhet ska patienter och personal vara säkert identifierade.

Unik identitet ska införas i elektroniska patientinformationssystem för att beteckna personal och utgörs av HSA-ID, identitet konstruerad utifrån nationella riktlinjer i Hälso- och Sjukvårdens Adressregister. Denna är en global unik identitet, som byggs upp av beteckning för Sverige,

Region Skånes organisationsnummer och ett löpnummer. Identiteten måste kunna verifieras elektroniskt på ett säkert sätt med Region Skånes ID-kort.

Som unik identitet på patient utnyttjas personnummer. Om personnummer saknas ska gällande regler för reservnummeranvändning i Region Skåne följas (*Personnummerhantering i HoS, PM 2003*).

Tillgång till patientinformation

Tillgång till patientinformation inom Region Skåne betraktas som ett inhämtande av patientinformation och inte ett utlämnande enligt sekretesslagen. Patientinformationen är dock alltid skyddad av sekretess.

Att ta del av uppgifter för kvalitetsgranskning över förvaltningsgränser inryms under patientdatalagens syfte med en patientjournal. Verksamheter som blir berörda av sådana uttag av information ska dock informeras.

Patienten kan motsätta sig att journaluppgifter inom sekretessområdet blir elektroniskt tillgängliga för andra vårdenheter eller vårdprocesser där patienten vårdas och då ska uppgifterna spärras. Denna inre spärr kan hävas om patienten uttalar detta eller om samtycke inte kan inhämtas och informationen kan antas ha betydelse för oundgänglig vård i en nödsituation. Uppgift om eventuell spärr ska vara tillgänglig för andra vårdenheter.

Utlämnande av patientinformation

Utlämnande av patientinformation kan göras genom direktåtkomst vid sammanhållen journalföring eller genom utlämnande efter sedvanlig sekretessprövning.

Direktåtkomst genom sammanhållen journalföring

En överenskommelse mellan Region Skåne och en eller flera andra vårdgivare, möjliggör att direktåtkomst kan ske till journaluppgifter hos parterna. Patienten skall informeras om sammanhållen journalföring, när sådan föreligger. Vid sammanhållen journalföring ska framgå att det finns ospärrade respektive spärrade uppgifter hos annan vårdgivare.

Patienten ska ge sitt samtycke till hälso- och sjukvårdspersonal som behöver ta del av patientinformation hos annan vårdgivare i sammanhållen journalföring. Samtycke avges vanligen i direkt anslutning till vård, men kan även ges i förväg vid planerade och konkreta vårdssituationer. Exempel på sådana situationer är remisser och samordnad vårdplanering.

Patienten kan motsätta sig att hans/hennes journaluppgifter ingår i den sammanhållna journalföringen och då ska en spärr upprättas. Om spärr föreligger vid sammanhållen journalföring, kan vid nödsituation spärren hävas av den vårdgivare som lagt den. Rutiner för detta ska vara överenskomna.

Direktåtkomst för patient

Patientdatalagen medger möjlighet för vårdgivaren (Region Skåne) att bereda patienten direktåtkomst till viss del av sina egna journaluppgifter förutsatt att ett utlämnande kan göras enligt sekretesslagen. Om Region Skåne väljer att begränsa direktåtkomst för patient ska han eller hon informeras om detta. Likaså ska patient informeras om varthän han eller hon kan vända sig för att få hjälp med att förstå uppgifterna.

Patienten kan också via direktåtkomst få uppgifter om vem som berett sig tillgång till hans eller hennes elektroniska journal (logguppgifter). Patients direktåtkomst kräver dock att han eller hon har identifierats genom stark autentisering.

Annat utlämnande

Patient kan även idag i offentlig sjukvård få tillgång till sin journalinformation liksom logguppgifter men då genom ett formellt utlämnande i enlighet med tryckfrihetsförordningen. Ett sådant utlämnande av journaluppgifter ska föregås av sekretessprövning.

Patient kan också få tillgång till sina personuppgifter i vården genom ett registerutdragsförfarande en gång årligen enligt personuppgiftslagen.

Styrning av åtkomst via aktivt val

Alla steg vid elektronisk åtkomst av patientuppgifter ska föregås av att behörig användare gör ett aktivt val, dvs tar ställning till om han eller hon har rätt att ta del av uppgifterna. Detta gäller all tillgång till/åtkomst av patientuppgifter. Ett aktivt val ska alltid loggas.

Styrning av behörighet – rättighetstilldelning

Tilldelning av behörighet ska föregås av en behovs- och riskanalys. Rutiner för tilldelning, förändring och borttagning av behörigheter ska finnas.

Åtkomst/tillgång till patientinformation ges av verksamhetschef/motsvarande till den personal han eller hon ansvarar för. Vid ekonomiuppföljning eller annan administrativ verksamhetsuppföljning av patientinformation ska förvaltningschef tillse att det finns rutiner för rättighetstilldelning. Tillgångens art - läsa, skriva, skriva ut, ändra etc - och typ av patientinformation bestäms av arbetsuppgifterna. Dock får vid sammanhållen journalföring endast läsning ske.

Kontroll av åtkomst - uppföljning

Då behovet av tillgång till patientinformation ej går att avgöra fullt ut i förväg, är uppföljning nödvändig för att kunna tillse att tillgång/åtkomst till patientinformation utnyttjas enligt fastställda tillämpningsanvisningar. Detta ställer krav på registrering/loggning av vad som händer med patientinformationen.

Registrering/loggning av händelser ska kunna påvisa

- vem som har berett sig tillgång till patientinformation
- vilken patientinformation som har använts
- vad som har gjorts med patientinformationen och
- när dessa händelser har påbörjats och avslutats samt
- vid vilken vårdenhet händelserna har skett.

Genomförda kontroller av logguppgifter ska dokumenteras. Logguppgifter ska sparas i minst tio år.

Uppföljningen ska ske regelbundet och strukturerat samt riktat vid misstanke om eller risk för överträdelse av författningar på området. Urval för uppföljning av personal och patienter ska vara baserat på bestämda kriterier eller ske slumpmässigt. Omfattningen på uppföljningen ska innebära att en personals aktiviteter med patientinformation blir granskade slumpmässigt över året med automatiska och manuella rutiner.

Den information som ska lämnas till patient om åtkomsten till hans eller hennes patientuppgifter ska tydligt visa från vilken vårdenhet och vid vilken tidpunkt någon har berett sig tillgång till uppgifterna. Informationen ska vara tydligt utformad så att patient kan avgöra om åtkomsten har varit befogad eller inte.

Vid överträdelse av författningar skall åtgärder enligt Region Skånes vägledning vid dataintrång följas.

Säkerhetskopiering

Rutiner för säkerhetskopiering av patientuppgifter ska finnas och utvisa hur ofta sådan sker, hur länge säkerhetskopior sparas samt hur ofta återläsningstester görs. Därutöver ska finnas rutiner för säker hantering och förvaring av säkerhetskopior.

Ansvar

Inom vårdgivaren Region Skåne finns olika typer av ansvar beroende på hur patientinformationen hanteras.

Personuppgiftsansvar

Hantering av patientinformation innebär i allmänhet behandling av personuppgifter enligt personuppgiftslagen. Regionstyrelsen är personuppgiftsansvarig för all behandling av personuppgifter i regionens verksamheter och även för personuppgifter som görs tillgängliga genom sammanhållen journalföring. Det innebär att när vårdgivaren Region Skåne deltar i sammanhållen journalföring och bereder sig tillgång till personuppgifter hos andra vårdgivare åläggs regionen också ett ansvar för att åtkomsten och hanteringen av uppgifterna följer reglerna i PDL.

Tjänsteägares ansvar

Tjänste-/systemägare ansvarar för att patientinformationssystemet är utformat så att skydd mot förvanskning finns genom funktioner för signering, läsning och versionshantering.

Verksamhetschefs ansvar

Verksamhetschef/motsvarande ansvarar för att

- tillgång/åtkomst till patientinformation ges och att utdelade behörigheter för åtkomst till patientuppgifter är ändamålsenliga och förenliga med hälso- och sjukvårdspersonalens och andra befattningshavares aktuella arbetsuppgifter samt att utnyttjandet av patientinformation följs upp. Ansvaret omfattar därmed personalens tillgång till patientinformation såväl vid den egna vårdenheten som hos vårdgivaren i övrigt samt personalens tillgång till patientinformation hos annan vårdgivare.
- patients identitet hanteras enligt *Personnummerhantering i HoS* och att personal hanteras med HSA-ID och Region Skånes ID-kort
- information om hur tillgång till/utlämnande av patientinformation och uppföljning går till, ges till patient och personal.

Journalförarens ansvar

Ansvar för innehållet i journalen åvilar den som svarar för uppgifterna och kvarstår hos densamme även om journaluppgifterna blir tillgängliga för andra vårdgivare.

Termer och definitioner

Autentisering	Kontroll av uppgiven identitet
Direktåtkomst	Annan vårdgivare eller patient får på elektronisk väg direkt tillgång till information hos en vårdgivare endast genom att läsa informationen.
Elektronisk åtkomst	Elektronisk tillgång till vårdinformation inom ett sekretessområde
Informationsbärare	Papper, videoband, ljudband, CD, DVD, dataminne, server
Patientrelation	Uppstår när personal deltar i vården och utför eller ansvarar för patientrelaterade aktiviteter (planera, utföra eller utvärdera)
Sammanhållen journalföring	Flera vårdgivare kan ge och få direktåtkomst till varandras elektroniska journalhandlingar om de uppfyller PDL:s krav. Deltagande i sammanhållen journalföring samt vilka uppgifter som ska göras tillgängliga ska vara överenskommet mellan berörda vårdgivare.
Spärr	Patients möjlighet att motsätta sig att journaluppgift görs tillgänglig på elektronisk väg inom vårdgivaren och mellan vårdgivare. Spärr kan bara initieras av patienten, ej av vårdgivaren.
Stark autentisering	Kontroll av uppgiven identitet med e-legitimation.
Verksamhetschef	Av Socialstyrelsen författningsreglerad befattningshavare med ansvar för hälso- och sjukvårdsverksamhet. Motsvaras i tandvården av klinikchef samt i habilitering och hjälpmedel av enhetschef.
Vårdenhet	Organisatorisk enhet som tillhandahåller hälso- och sjukvård och definieras av det område som en verksamhetschef ansvarar för. Ex: Vårdcentral, klinik, mottagning, vårdavdelning.
Vårdgivare	Statlig myndighet, landsting och kommun i fråga om sådan hälso- och sjukvårdsverksamhet som myndigheten, landstinget eller kommunen har ansvar för (offentlig vårdgivare) samt annan juridisk person eller enskild näringsidkare som bedriver hälso- och sjukvårdsverksamhet (privat vårdgivare)
Vårdinformation	Patientrelaterade uppgifter i t ex journal-/laboratorie-/patientadministrativt-/röntgensystem
Vårdprocess	En följd av aktiviteter eller åtgärder som utförs för en patient, avseende ett visst hälsoproblem, hos en vårdgivare. Begreppet kan också innefatta ett i förväg definierat samarbete.

Fastställes 2009-05-28



Sören Olofsson
Regiondirektör