

LANDSTINGS- REVISORERNA

Projektrapport
Nr 21/20009

Patientjournalssystemet TakeCare – uppföljning av tidigare granskning

- Sedan patientdatalagen infördes har ett antal åtgärder vidtagits för att TakeCare, som används inom stora delar av vården, ska nå upp till lagens intentioner. Arbete pågår fortfarande men journalsystemet uppfyller inte till alla delar patientdatalagens krav.
- Landstingsstyrelsen bör tydliggöra den övergripande organisationen och ansvarsfördelningen för journalsystemet TakeCare.
- Landstingsstyrelsen bör säkerställa att SLL:s IT-säkerhetsriktlinjer liksom SLL förvaltningsmodell stöder utvecklingen av en sammanhållen patientjournal.
- De sjukvårdsproducenter som använder TakeCare måste
 - säkerställa att systemet uppfyller patientdatalagens samtliga krav och Socialstyrelsens föreskrifter
 - tillse att informationssäkerhetsfrågorna som rör systemet ingår i respektive vårdorganisations ledningssystem
 - inrätta en för deltagande vårdgivare gemensam funktion med ansvar för att bevaka informationssäkerhetsfrågorna för systemet
 - dokumentera en rutin för att årligen och oberoende av händelser genomföra säkerhetsgranskningar.

Styrelserna för
Karolinska Universitetssjukhuset
Danderyds sjukhus AB
Södertälje sjukhus AB
S:t Eriks Ögonsjukhus AB
Stockholms läns sjukvårdsområde

Rapport 21/2009 Patientjournalssystemet TakeCare – uppföljning av tidigare granskning

Revisorerna i revisorsgrupp II beslutade på möte 2010-03-18 överlämna rapporten till styrelserna för Karolinska Universitetssjukhuset, Danderyds sjukhus AB, Södertälje sjukhus AB, S:t Eriks Ögonsjukhus AB och Stockholms läns sjukvårdsområde för yttrande senast 2010-06-18.

Paragrafen justerades omedelbart.

Härmed överlämnas rapporten.



Göran Hammarsjö
ordförande



Agneta Fohlström
sekreterare

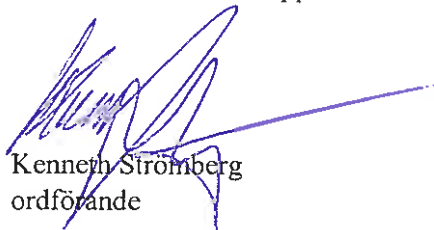
Landstingsstyrelsen


Rapport 21/2009
Patientjournalssystemet TakeCare – uppföljning av tidigare granskning

Revisorerna i revisorsgrupp I beslutade på möte 2010-03-26 överlämna rapporten till landstingsstyrelsen för yttrande senast 2010-06-18.

Paragrafen justerades omedelbart.

Härmed överlämnas rapporten.


Kenneth Strömberg
ordförande


Agneta Fohlström
sekreterare

INNEHÅLL

1. SLUTSATSER OCH REKOMMENDATIONER.....	1
2. UTGÅNGSPUNKTER FÖR GRANSKNINGEN	2
2.1 Motiv för granskningen.....	2
2.2 Avgränsning	3
2.3 Revisionskriterier.....	3
2.4 Metod	3
3. GRANSKNINGENS RESULTAT	3

Bilaga:

Meile AB:S rapport ”Uppföljning av rekommendationer från 2007 års granskning av patientjournalssystemet TakeCare”

1. Slutsatser och rekommendationer

I 2007 års revision gjordes en fördjupad granskning av IT-systemet för patientjournalhantering, TakeCare, som avrapporterades i årsrapporten för landstingsstyrelsen. I rapporten framfördes flera rekommendationer. Det gällde följsamhet gentemot den kommande patientdatalagen, hanteringen av informationssäkerhetsfrågor m.m. I 2009 års revision har en uppföljande granskning genomförts utifrån framförda rekommendationer. Därutöver har översiktligt granskats förvaltningsorganisationen för TakeCare avseende informationssäkerhet.

Syftet med patientdatalagen, som gäller från den 1 juli 2008, är att informationshanteringen och journalföringen inom hälso- och sjukvården inklusive tandvården ska vara organiserad så att den tillgodoser patientsäkerhet och god kvalitet samtidigt som kostnadseffektiviteten främjas.

Den uppföljande granskningen visar att systemägaren har bedrivit ett omfattande arbete för att bedöma vad patientdatalagens krav innebär och hur dessa frågor ska hanteras i TakeCare. Sedan lagen infördes har ett antal åtgärder vidtagits för att nå upp till lagens intentioner. Trots detta uppfyller journalsystemet inte till alla delar patientdatalagens krav. Det gäller bl.a. krav på kryptering och stark autentisering (kontroll av uppgiven identitet).

Vidare är informationssäkerhetsarbetet inte optimalt i den meningen att det inte har någon fast form och tydliga rutiner att följa. Konsekvensen kan bli att vissa risker inte belyses. Det saknas en tydlig koppling till vårdgivarnas ledningssystem och en tydlig funktion för informationssäkerhets- och riskhantering för att säkerställa ett kontinuerligt säkerhetsarbete. Det föreligger också en otydlighet kring TakeCares organisation och ansvarsfördelning vilket kan ge upphov till frågor och missförstånd.

Utifrån genomförd granskning lämnas följande rekommendationer:

- Landstingsstyrelsen bör säkerställa att SLL:s IT-säkerhetsriktlinjer liksom SLL förvaltningsmodell stöder utvecklingen av en sammanhållen patientjournal.
- Landstingsstyrelsen bör tydliggöra den övergripande organisationen och ansvarsfördelningen för patientjournalssystemet TakeCare.

De sjukvårdsproducenter som använder TakeCare måste

- säkerställa att patientjournalssystemet TakeCare uppfyller patientdatalagens samtliga krav och Socialstyrelsens föreskrifter
- tillse att informationssäkerhetsfrågorna som rör patientjournalssystemet TakeCare ingår i respektive vårdorganisations ledningssystem
- inrätta en för deltagande vårdproducenter gemensam funktion med ansvar för att bevaka informationssäkerhetsfrågorna för patientjournalssystemet TakeCare
- dokumentera en rutin för att årligen och oberoende av händelser genomföra säkerhetsgranskningar.

2. Utgångspunkter för granskningen

2.1 Motiv för granskningen

I samband med sammanslagningen av Huddinge Universitetssjukhus och Karolinska sjukhus beslöt sjukhusdirektören att patientjournalssystemet TakeCare skulle utgöra ett enhetligt stöd för vårdadministration och vårddokumentation inom det sammanslagna sjukhuset.

I 2007 års revision gjordes en fördjupad granskning av TakeCare som avrapporterades i årsrapporten för landstingsstyrelsen. I årsrapporten framfördes flera rekommendationer. Det gällde om patientjournalssystemet TakeCare är i paritet med nuvarande lagstiftning vad avser utlämnande av journalinformation, sekretessgränser, möjligheter att anpassa till den förväntade nya patientdatalagen, i linje med nationella IT-strategin för vård och omsorg samt långsiktig funktionalitet. Vidare framfördes att en säkerhetsinriktad genomgång borde göras av redan befintliga installationer av TakeCare. Det gällde fysisk säkerhet, skyddet av information, behörighets- och loggkontroll, säkerhetskopiering, kryptering m.m.

TakeCare används inom stora delar av hälso- och sjukvården i SLL. Systemet används även av en del privata vårdgivare som landstinget har avtal med. Följande verksamheter inom landstinget använder journalssystemet: Karolinska Universitetssjukhuset, Danderyds sjukhus AB, Södertälje sjukhus AB, S:t Eriks Ögonsjukhus AB och SLSO. Under 2010 planerar resterande delar av vården att införa TakeCare.

Det har bildats en gemensam systemägarorganisation¹ som leds av en styrelse, ”Samverkan för TakeCare”. Ledamöterna utses av respektive förvaltningschef för de ingående parterna. Projekt för drift och utveckling m.m. initieras av styrelsen och genomförs sedan av ”Centrum för Samverkan TakeCare” som är en resultatenhet inom Karolinska Universitetssjukhusets organisation. Avtal har tecknats mellan de inblandade parterna.

Till ledning för verksamheten har utsetts en chef som även är systemägare för TakeCare. För det operativa arbetet på central nivå finns även en stab. Därutöver finns lokal systemförvaltning av TakeCare i de ingående organisationerna.

Vid granskningen i 2007 års revision fanns inte systemägarorganisationen eller ”Centrum för Samverkan TakeCare”.

I 2009 års revision har en uppföljande granskning genomförts utifrån framförda rekommendationer i årsrapporten för landstingsstyrelsen 2007. Därutöver har

¹ Karolinska, SLSO, Södertälje sjukhus AB, HSF Gotland, Stiftelsen Stora Sköndal, St Eriks Ögonsjukhus AB, Nynäs Vård AB, Rehabstation Stockholm AB, Liljeholmsmottagningen, Sophiahemmet m.fl.

översiktligt granskats förvaltningsorganisationen för TakeCare avseende informationssäkerhet.

2.2 Avgränsning

En rättsprocess pågår för närvarande angående om spridningen av TakeCare till nya organisationer i vården ska vara föremål för upphandling eller inte. Länsrätten i Stockholm har i en dom i september 2009 beslutat att SLSOs direktupphandling av journalsystem ska göras om. Domstolen ansåg att upphandlingen genomförts i strid mot LOU. SLL har överklagat domslutet och ärendet ligger sedan i oktober 2009 hos Kammarrätten. Granskning av upphandlingen av TakeCare ingår inte i granskningen.

2.3 Revisionskriterier

Granskningen har utgått från bl.a. följande revisionskriterier:

- Patientdatalagen (2008:355)
- Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården
- SLLs Informationssäkerhetspolicy och Riktlinjer för informationssäkerhet
- Den nationella IT-strategin,
- SS-ISO IEC 27001 - 2006 – Ledningssystem för informationssäkerhet

2.4 Metod

Granskningen har utförts genom studier av relevant dokumentation. Intervjuer har genomförts med bl.a. systemägare, informationsägare, IT-direktör, teknikchef SLL-IT, användare, informationssäkerhetschef, koncernsamordnare IT, landstingets chefsjurist, lokal IT-chef, lokal systemägare, lokal systemförvaltare, IT-säkerhetsansvarig SLL-IT och projektledare för 8-projektet. Intervjuer har även genomförts med representant för leverantören, Socialstyrelsen och Datainspektionen.

Projektledare för granskningen har varit Susanne Kangas. Granskningen har utförts med konsultstöd av Meile AB.

3. Granskningens resultat

Informationshanteringen inom hälso- och sjukvården ska enligt patientdatalagen, som infördes den 1 juli 2008, vara organiserad så att den tillgodoser patientens säkerhet och gör det möjligt för vårdgivaren att erbjuda en kostnadseffektiv vård av god kvalitet. Vårdgivaren ansvarar för att ledningssystemet för kvalitet och patientsäkerhet behandlar informationssäkerhetsarbetet. Vårdgivaren ska också säkerställa att ledningssystemet omfattar de rutiner som krävs för att uppfylla kraven i landstingets informationssäkerhetspolicy och riktlinjer för informationssäkerhetsarbetet.

Av landstingets Vård-IT-plan framgår att ”SLL ägda förvaltningar/bolag har ett gemensamt huvudjournalsystem. Systemet är TakeCare förutsatt att det kan beslutas inom ramen för upphandlingslagstiftningen. Krävs upphandling så ska

ett gemensamt system upphandlas och införs.” Ärendet har föredragits för Strategiska utskottet 2008.

Under 2009 har landstingsdirektören angett att TakeCare ska utgöra huvudalternativet för val av journalsystem inom landstinget, vilket har påverkat utvecklingen. Idag hanteras ca 2,2 miljoner patientjournaler i systemet.

Den uppföljande granskningen har genomförts av Meile AB och redovisas i sin helhet i bilagd rapport. Den uppföljande granskningen visar att systemägaren har bedrivit ett omfattande arbete för att bedöma vad patientdatalagens krav innebär och hur dessa frågor ska hanteras i TakeCare. Sedan lagen infördes har ett antal åtgärder vidtagits för att nå upp till lagens intentioner. Trots detta uppfyller journalsystemet inte till alla delar patientdatalagens krav. Det gäller bl.a. kryptering och stark autentisering (kontroll av uppgiven identitet).

Konsulten bedömer att arbetet med att skapa TakeCare för en sammanhållen journalföring i sina huvuddrag är i linje med den nationella IT-strategin.

Säkerhetsgranskningar har genomförts av den centrala systemförvaltningen för TakeCare. Det har dels skett under 2008, dels efter avbrottet i december 2008. Granskningarna har bl.a. omfattat administrativa rutiner, fysiskt skydd och logiskt skydd. Konsulten efterlyser dock en dokumenterad rutin för att årligen och oberoende av händelser genomföra säkerhetsgranskningar.

Trots avsaknad av regelrätt analys liksom en ingående funktionell jämförelse mellan olika journalsystem förefaller flertalet av de intervjuade anse att TakeCare tillgodoser vårdens behov av journalsystem. Utveckling pågår dessutom kontinuerligt för att anpassa och förbättra systemet.

Ansvar för informationssäkerhet är enligt landstingets riktlinjer för informationssäkerhet fördelat på flera roller. Informationsägaren har ansvar bl.a. för att riskanalyser genomförs och att de samordnas med andra informationsägare. Systemägaren har bl.a. ansvar för att specificera skyddsnivån genom instruktioner, vidta åtgärder utifrån riskanalyser m.m. När det gäller TakeCare är informationsägarskapet uppdelat på ett stort antal personer, ca 200 personer. Någon central representant för informationsägarna finns inte.

SLLs styrdokument såsom IT-säkerhetsriktlinjer och förvaltningsmodell innehåller inte helt anpassade strukturer för sammanhållen journalföring. Det är systemägaren som vidtar lämpliga åtgärder i den egna systemförvaltningen för att organisera informationssäkerhetsarbetet.

Den organisation och ansvarsfördelning som finns kring TakeCare är inte enkelt överblickbar. Innebörden i roller och ansvar mellan de av parterna slutna avtalen och kopplingarna till SLLs IT-förvaltningsmodell och SLLs riktlinjer för informationssäkerhet behöver förtydligas.

2010-03-21

**Uppföljning av rekommendation
från 2007 års granskning
av patientjournalssystemet
TakeCare**

Hornsgatan 51, 118 49 Stockholm

Tel nr 08-556 07 690 Mobil tfn 070 - 535 01 85 Fax 08 – 556 07 691
E-post g.hagnemark@meile.se

Innehåll

1. Utgångspunkter för uppföljningen	3
1.1 Uppföljning av lämnade rekommendationer	3
1.2 Bakgrund	4
1.3 Organisation och ansvar	4
2. Metod	5
3. Resultat.....	6
3.1 Sammanfattande bedömning	6
3.2 Har analys gjorts av om TakeCare följer lagstiftningen?	8
3.3 Har analys gjorts av om TakeCare är i linje med den nationella IT-strategin för vård och omsorg?	13
3.4 Har analys gjorts av om TakeCare är långsiktigt funktionellt?.....	14
3.5 Har en säkerhetsgranskning genomförts?	16
3.6 Har analys gjorts av hur SLL tillgodoser vårdens behov av journalsystem?.....	18
3.7 Har analys gjorts av om åtgärder är i linje med SLLs IT-strategi?	20
3.8 Är CSTCs funktion för informationssäkerhet ändamålsenlig?	20

1. Utgångspunkter för uppföljningen

1.1 Uppföljning av lämnade rekommendationer

Journalssystemet TakeCare (TC) som ursprungligen utvecklades inom Huddinge sjukhus mellan 1996 och 2002 har under senare år fått stor spridning och används idag inom större delen av vården i Stockholms läns landsting (SLL). Landstingsrevisorerna SLL gjorde under 2007 en fördjupad granskning av TC som avrapporterades i årsrapport 2007 för Landstingsstyrelsen. Revisorerna lämnade i den granskningen ett antal rekommendationer:

Uppdraget omfattar att belysa om följande rekommendationer följts.

A/ att systemägaren genomför en analys av om TakeCare är

- i paritet med nuvarande lagstiftning vad avser utlämnande av journalinformation, sekretessgränser etc.
- anpassningsbart till den förväntade nya patientdatalagen
- i linje med nationella IT-strategin för vård och omsorg
- långsiktigt funktionellt

B/ att systemägaren och respektive informationsägare genomför en riktad säkerhetsgranskning av redan befintliga installationer vad beträffar skyddet av information, både vad avser

- administrativa rutiner (t.ex. behörighets- och loggkontroll)
- fysisk säkerhet (t.ex. säker driftmiljö, tillgängliga och användbara säkerhetskopior)
- logiskt skydd (t.ex. behovet av kryptering).

C/ En förutsättningslös analys av hur Stockholms läns landsting bäst tillgodoser vårdens behov av journalssystem och att planerade och vidtagna åtgärder är i linje med den kommande IT-strategin.

D/ Därutöver ingår i uppdraget att granska den funktion Centrum för Samverkan Take Care (CSTC) har avseende informationssäkerhet för TakeCare. CSTC är den organisation till vilken ägarna, Karolinska, STS AB, SLSO och Hälso- och sjukvårdsförvaltningen på Gotland, via samverkansavtal har delegerat ansvaret för systemägarskapet.

Detta är en uppföljande granskning som inriktas på tidigare rekommendationer. Förändringar har emellertid i viss mån skett i förutsättningarna sedan nämnda rekommendationer formulerades. Därför har denna uppföljning också anpassats till dessa förhållanden. Bl.a annat har det då aktuella landstingsövergripande projektet Gemensam Vårdokumentation (GVD) lagts ned. Därför har en av rekommendationerna som avsåg nämnda projekt också utgått ur uppföljningen. Men å andra sidan har en ny förvaltningsorganisation skapats kring TC, varvid en granskning av i huvudsak dess roll för informationssäkerhet ingår i detta uppdrag.

Ytterligare förändringar har skett i miljön kring TC och dessa behandlas i fortsättningen den mån det bedöms vara relevant för uppföljningen.

1.2 Bakgrund

TC är en produkt som ägs av företaget Profdoc Care AB. Företaget har f.n tre kunder (installationer); Karolinska, TioHundra AB och Stockholms sjukhem. Denna granskning avser endast den förstnämnda, d.v.s. karolinskas installation.

TC har sedan 1997 varit i drift vid Huddinge sjukhus (HS), numera Karolinska. Systemägarskapet för denna installation togs vid skapandet av den sammanslagna sjukhusorganisationen över av Karolinska. Av nyttjandeavtalet som Karolinska övertagit framgår att "HS innehar en icke-exklusiv och tidsobegränsad licens att nyttja TakeCare, för ett obegränsat antal användare och installationer inom HS organisation vari förutom HS även ingår dotterbolag till HS, vårdgivare med vilka HS har vårdssamarbete, samt sjukvården Gotland".

Med tiden har ytterligare organisationer såsom enheter i Stockholms läns sjukvårdsområde (SLSO) m.fl. beslutat sig för att nyttja TC och ingår numer bland dem som är anslutna till Karolinskas installation av TC. När Karolinskas installation omnämns i fortsättningen omfattas flera organisatoriska ägare¹.

1.3 Organisation och ansvar

Under 2008 valde dessa parter att för Karolinskas installation inrätta och genom avtal formalisera en särskild Samverkan för TC (STC) (Avtal samverkan om TakeCare). Denna innebär att man för karolinskas installation bildade en gemensam systemägarorganisation. Den inordnades juridiskt och ekonomiskt som en sluten resultatenheter i Karolinskas organisation. Enligt avtalet ingår STC i Karolinska men utgör en självständig del med egen ekonomi och leds av en styrelse enligt beslut fattat av sjukhusdirektören. Relationen mellan parterna regleras i avtal. De deltagande organisationerna ska bidra till helheten genom att insatser görs lokalt efter samordning centralt. Det innebär att projekt för drift och utveckling m.m. initieras och planeras centralt, medan praktiskt arbete utförs lokalt. Ledamöterna till styrelsen (tjänstemän) utses av respektive förvaltningschef inom de ingående parterna.

Till stöd för STC att genomföra de centrala funktionerna har skapats en gemensam systemägarorganisation CSTC. Den utgör en central förvaltningsorganisation, styrd via STC d.v.s. representanter för de ingående organisatoriska ägarna. Till ledning för verksamheten har en centrumchef utsetts för CSTC på delegation från STC. Flera grupper med principiella uppgifter finns som stöd för arbetet bl a en policygrupp och en systemrättsägargrupp. För det operativa arbetet på central nivå finns en stab knuten till CSTC. Därtill kommer lokal TakeCare-förvaltning vid de ingående organisationerna och alla användare.

¹ Exempelvis, Karolinska, SLSO, Södertälje sjukhus AB, HSF Gotland, Stiftelsen Stora Sköndal, St Eriks Ögonsjukhus AB, Nynäs Vård AB, Rehabstation Stockholm AB, Liljeholmsmottagningen, Sophiahemmet.

Vissa arbetsuppgifter är av den storleken att de sammanförts till särskilda projekt vilka bemannats från CSTC, de berörda vårdgivarna, SLL-IT och leverantören ProfDoc Care AB. Centrumchefen för CSTC är systemägare för TC.

När föregående granskning rapporterades 2008-03-13 fanns således inte STC. Därmed är det rimligt att de rekommendationer som granskningen då lämnade till systemägaren idag får anses vara riktade till STC och i förlängningen till styrelserna för respektive part i STC.

Beroende på vilken karaktär som en fråga om ansvar har kan den komma att få olika adressering inom partskollektivet. Rör det sig om patientsäkerhetsrelaterade frågor ligger ansvaret på respektive part, d.v.s. vårdgivare. Rör det sig om förvaltningsrelaterade frågor som ekonomi, personal, lokaler, utrustning, avtal m.m. torde ansvaret helt ligga på Karolinskas ledning mot bakgrund av att enheten där har sin ekonomiska och juridiska hemvist. Att det sannolikt föreligger en sådan fördelning av ansvarstagandet och hur det i så fall ser ut finns emellertid inte beskrivet i något dokument.

Finansieringen av systemförvaltningen sker genom att parterna erlägger en avgift per årlig användare av TC. Dessa medel erläggs från respektive part till Karolinska där de redovisas på ett separat kostnadsställe och ingår i den samlade omslutningen. I avgiften ingår kostnaden för CSTC, drift vid SLL-IT och av förvaltningen beställda utvecklingsinsatser hos leverantören.

Denna uppföljning avser enbart Karolinskas installation med förvaltningsenheten CSTC som också är den enskilt största kunden till Profdoc Care AB. Till CSTC var i början av 2010 ett drygt tiotal sjukhus och vårdenheter anslutna. Totalt representerar de 25 000 anställda och ca 2,2 miljoner patientjournaler.

En rättsprocess pågår f.n. angående TC. Den avser huruvida spridningen av systemet till nya vårdgivare ska vara föremål för upphandling eller ej. Eftersom processen pågår behandlas den inte i denna uppföljning.

2. Metod

Granskningen har utförts genom studier av relevant dokumentation och intervjuer med ett urval ansvariga personer samt i övrigt berörda personer för att skapa en bild av TC och hanteringen av systemet.

Intervjuer har genomförts med personer inom Stockholms läns landsting med bl.a systemägare, informationsägare, IT-direktör, teknikchef SLL-IT, användare, informationssäkerhetschef, koncernsamordnare IT, landstingsjurist, lokal IT-chef, ägare SLSO, lokal systemförvaltare, IT-säkerhetsansvarig SLL-IT och projektledare 8-projektet.

Intervjuer och kontakter har hållits med personer utanför SLL som representerar leverantören, Socialstyrelsen och Datainspektionen.

3. Resultat

3.1 Sammanfattande bedömning

Rekommendation

att systemägaren genomför en analys av om TakeCare är

- *i paritet med nuvarande lagstiftning vad avser utlämnande av journalinformation, sekretessgränser etc.*
- *anpassningsbart till den förväntade nya patientdatalagen*
- *i linje med nationella IT-strategin för vård och omsorg*
- *långsiktigt funktionellt*

Bedömning

Systemägaren har initierat och bedrivit ett intensivt analysarbete avseende hur TC uppfyller eller inte uppfyller lagstiftningen. Trots detta och ett omfattande åtgärdsarbete uppfyller TC efter drygt ett och ett halvt år fortfarande till vissa delar inte Patientdatalagen (2008:355). Det gäller t ex kryptering och stark autenticering.

Någon analys av om TC ligger i linje med den nationella IT-strategin för vård och omsorg som resulterat i ett enhetligt dokument har systemägaren inte tagit fram. Arbetet med att skapa TC för en sammanhållen journalföring är emellertid i sina huvuddrag i linje med den nationella IT-strategin.

Systemägaren har inte gjort någon analys av om TC är långsiktigt funktionellt som resulterat i form av ett enhetligt dokument. Avsaknaden av ett dokument med en samlad analys innebär emellertid inte per automatik att någon analys överhuvud taget inte har gjorts. De åtgärder som vidtagits visar på ett kontinuerligt arbete med att överväga lämpliga sätt för att säkra att TC blir långsiktigt funktionellt. En samlad analys hade emellertid ökat tydligheten och gett beslutsfattarna bättre möjlighet till avvägningar mellan olika handlingsvägar.

Rekommendation

att systemägaren och respektive informationsägare genomför en riktad säkerhetsgranskning av redan befintliga installationer vad beträffar skyddet av information, både vad avser

- *administrativa rutiner (t.ex. behörighets- och loggkontroll)*
- *fysisk säkerhet (t.ex. säker driftmiljö, tillgängliga och användbara säkerhetskopior)*
- *logiskt skydd (t.ex. behovet av kryptering).*

Bedömning

Säkerhetsgranskningar har initierats av den centrala förvaltningen för TC som en gemensam aktivitet för karolinskas installation vilken samverkan inom STC avser. Det har dels skett i ett initialt skede 2008, dels på förekommen anledning efter avbrottet 2008-12-18.

Granskningarna har behandlat administrativa rutiner, fysiskt skydd och logiskt skydd om än i olika grad. Systemägaren har haft en tongivande roll i arbetet med att initiera säkerhetsgranskningarna.

När det gäller informationsägarnas deltagande i riskanalyserandet så har det inte skett bokstavligt. En förklaring kan vara att granskningar genomförts på central nivå och en annan att det tidigare rått viss oklarhet om vem som är informationsägare i TC. Detta är dock inte acceptabla skäl för att avstå från att genomföra säkerhetsgranskningar. Sådana borde ha genomförts inom varje vårdenhet vad avser skyddet för information inom just den verksamheten. Om det för den enskilde informationsägaren var oklart vad som låg i dennes ansvar borde CSTC ha informerat dem om detta.

Uppföljningsfrågan får med en strikt tolkning anses vara utförd för systemägarens del genom den aktivitet som gjordes 2008, medan den inte har utförts för informationsägarnas del.

Säkerhetsarbete utgör ett kontinuerligt arbete och det finns flera aktualiserade frågor kvar att lösa. Den säkerhetsgranskning som gjorts efter den första har varit knuten till den speciella händelsen, avbrottet 2008-12-18. Även om det också under 2009 gjorts en säkerhetsgranskning kan hanteringen inte anses vara tillfyllest eftersom det saknas en rutin för att årligen och oberoende av händelser genomföra granskningar. De ingår således inte i ett kontinuerligt säkerhetsarbete utan måste i ett processperspektiv betraktas som engångsföreteelser.

Rekommendation

En förutsättningslös analys av hur Stockholms läns landsting bäst tillgodoser vårdens behov av journalsystem och att planerade och vidtagna åtgärder är i linje med den kommande IT-strategin.

Bedömning

Någon förutsättningslös analys av hur SLL bäst skulle tillgodose vårdens behov av journalsystem finns inte dokumenterad från tiden efter granskningen. Det innebär dock inte att man avstått från att diskutera denna fråga och pröva olika alternativ. Den utveckling som lett fram till dagens situation har emellertid inte grundats på resultatet av en i efterhand identifierbar analys utan snarare på ett antal beslut och omständigheter som i olika grad bidragit till att förhållandena idag ser ut som de gör. På frågan om hur SLL bäst tillgodoser vårdens behov av journalsystem finns det därför inte något tydligt svar.

Trots avsaknad av regelrätt analys liksom en ingående funktionell jämförelse mellan olika journalsystem förefaller den uppfattning som flertalet av de intervjuade förfäktar vara att TC, inkluderande synpunkter på detsamma, tillgodoser vårdens behov av journalsystem.

Utveckling pågår därtill kontinuerligt för att anpassa och förbättra systemet.

Rekommendation

Därutöver ingår i uppdraget att granska den funktion Centrum för Samverkan Take Care (CSTC) har avseende informationssäkerhet för TakeCare. CSTC är den organisation till vilken ägarna, Karolinska, STS AB, SLSO och Hälso- och sjukvårdsförvaltningen på Gotland, via samverkansavtal har delegerat ansvaret för systemägarskapet.

Bedömning

Organisationsformen för CSTC har skapats för att ta tillvara hanteringen av många intressenter kring kärnan, den sammanhållna journalföringen. SLLs styrdokument såsom IT-säkerhetsriktlinjer och IT-förvaltningsmodell innehåller inte helt anpassade strukturer för sammanhållen journalföring. Mot den bakgrunden är det upp till systemägaren att tillsvidare

vidta lämpliga åtgärder i den egna systemförvaltningen för att organisera informationssäkerhetsarbetet och förbättra informationssäkerhetssamordnarnas och informationsägarnas kontaktytor i dessa frågor. I det här fallet kan det vara att inom CSTC inrätta en separat sammanhållande funktion för informationssäkerhet trots att en sådan inte finns anbefalld i SLLs centrala regelverk.

Den organisation och ansvarsfördelning som finns kring TC i övrigt är inte enkelt överblickbar. Innebörden i roller och ansvar mellan de av parterna slutna avtalen, SLLs IT-förvaltningsmodell och SLLs riktlinjer för informationssäkerhet ger inte en helt otvetydig bild.

Kopplingen mellan de berörda vårdgivarnas ledningssystem för kvalitet, enligt socialstyrelsens föreskrifter, och informationssäkerhetsarbetet i TC är inte tydlig. Kontaktytorna mellan ett system för sammanhållen journalföring och vårdgivarna blir naturligen många och kräver fastlagda och väl fungerande rutiner.

Sammantaget har CSTC arbetat med informationssäkerhet och vidtagit många viktiga åtgärder. Informationssäkerhetsarbetet är dock inte optimalt i den meningen att det inte har någon fast form och tydliga rutiner att följa. Konsekvensen kan bli att vissa risker inte belyses. Det saknas för att säkerställa ett kontinuerligt säkerhetsarbete såväl en tydlig funktion som väl beskrivna rutiner för informationssäkerhets- och riskhantering. Det föreligger också en otydlighet kring TC organisation och ansvarsfördelning som kan ge upphov till frågor och missförstånd.

3.2 Har analys gjord av om TakeCare följer lagstiftningen?

Iakttagelser

I det följande görs en kort genomgång av nio viktiga krav på förändringar som lagstiftningen inneburit samt hur status är för TC i dessa frågor vid denna uppföljning. Av rubriken framgår i vad mån TC för närvarande uppfyller lagen eller ej.

1/ Sekretessgränser: uppfyllt

Sekretessgränser är ett centralt begrepp vid utformningen av ett journalsystem. Det gäller gränser som avser såväl relationen vårdpersonal - patient som organisatoriskt inom och mellan *vårdgivare*.

Enligt Patientdatalagen får en användare till en patientjournal endast ta del av patientuppgifter som behövs för att han eller hon ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården. Därtill får användaren endast se de patientuppgifter som härrör från den egna *vårdenheten* eller den *vårdprocess* som användaren ingår i. För att få läsa ospärrade uppgifter vid andra vårdenheter eller vårdprocesser måste användaren göra ett aktivt val. För att få ta del av spärrade uppgifter krävs patientens samtycke. Vid nödsituationer får dock spärren brytas.

Enligt Patientdatalagen får det vid sammanhållen journalföring finnas möjlighet att ge eller få åtkomst till patientuppgifter hos en annan vårdgivare. Patienten har dock möjlighet att spärra sina uppgifter och motsätta sig en sammanhållen journalföring. I en sammanhållen journal ska det framgå om det finns ospärrade eller spärrade uppgifter

hos andra vårdgivare. För att en användare ska få ta del av ospärrade uppgifter om en patient vid en annan vårdgivare krävs att användaren; har en patientrelation, uppgifterna antas ha betydelse samt patientens samtycke. Är uppgifterna spärrade är huvudregeln att andra vårdgivare inte får ta del av sådana uppgifter. Patienten kan dock hos den vårdgivare som lagt in spärren begära att den hävs. Vid en nödsituation är det endast den vårdgivare som lagt in spärren som kan häva densamma.

De sekretessgränser som avser att användaren ska ha en vårdrelation till patienten och att informationen ska vara relevant för vårdsituationen bygger på en bedömning hos användaren. Hänsyn till dessa gränser ska tas genom användarens yrkeskunnande och goda omdöme. CSTC och vårdgivarna har fört en informationskampanj kring dessa frågor och de ingår i den introduktion som alla användare får.

För TC har sekretessgränser i enlighet med hur de stipuleras i Patientdatalagen byggts in i systemet vad gäller journalanteckningar. Gränserna går mellan vårdgivare och mellan vårdenheter. Verksamhetsindelningen är grunden för dessa gränser och inom SLL utgörs en vårdgivare av den som har ett eget organisationsnummer, medan en vårdenhet utgörs antingen av en klinik eller av en vårdcentral.

TC är i detta avseende anpassat efter lagen och SLLs definitioner av verksamheten. Det finns dock vårdgivare som nyttjar TC där verksamheten och journalsystemets struktur inte är helt anpassade till varandra. Det gäller vårdgivare som inte har organiserat sin verksamhet i enlighet med den struktur som lagen utgår från. Istället har de en matrisorienterad verksamhet. I en sådan struktur där vårdbehovet för patienten följer ett flöde till vilket personella insatser hämtas från olika vårdenheter efter behov kommer vårdenheternas gränser, och därmed sekretessgränser enligt Patientdatalagen, att ofta behöva överskridas. I sådana fall är organisationens arbetssätt inte i fullt samspel med journalsystemets uppbyggnad. Detta är ett problem som uppkommit i samband med att Södertälje sjukhus AB omorganiserades vid årsskiftet 2009/2010. Konsekvenserna av nämnda problem överblickas inte fullt ut ännu och än mindre vad som kan göras åt det. Vid beslut om att välja en ny organisationsform som innebär att verktyget inte står i samklang med förändringen torde det vara omorganisationen som är orsak till problemet och inte verktyget. Eventuell diskrepans gentemot lagstiftningen kvarstår dock att analysera och utgör legalt vårdgivarens ansvar.

En fråga som varit uppe till behandling under 2009/210 är huruvida Karolinska och SLSO är en gemensam eller två separata vårdgivare. Enligt SLLs tolkning av Patientdatalagen ska verksamheter med eget organisationsnummer utgöra en vårdgivare. Inom SLL definieras också verksamheter med eget organisationsnummer som bedriver hälso- och sjukvård inom landstinget finansierad av detsamma som vårdgivare. Socialstyrelsen har emellertid under 2009 initierat frågan om Karolinska och SLSO som utgör egna förvaltningsnämnder ska definieras som två särskilda vårdgivare trots att de har ett med landstinget centralt gemensamt organisationsnummer. Om så skulle vara fallet innebär det att TC inte uppfyller Patientdatalagen och att dessa båda organisationer måste skiljas åt som två vårdgivare i systemet. Landstingsdirektören har emellertid fastslagit sin ståndpunkt och fattat ett verkställighetsbeslut 2010-01 med innebörden att Karolinska och SLSO är en och samma vårdgivare.

2/ Visning av rättning, signaturer samt automatlåsning - uppfyllt

Socialstyrelsen har i sin tillsyn (dnr 08729/2006) avseende vårdgivaren Karolinska tagit upp brister med a/ visning av rättning i journaltext, b/ avsaknad av automatlåsning av journalanteckningar samt c/ ett fel i visningen av signaturer i läkemedelsadministreringsfunktionen. Karolinska har under hösten åtgärdat bristerna och redovisat detta för Socialstyrelsen. Socialstyrelsen har vid besök under slutet av 2009 konstaterat att bristerna är åtgärdade. Ärendet är därmed avslutat.

3/ Utlämnande av logginformation: uppfyllt

TC ger möjlighet att göra utskrifter av logginformation avseende vilka som haft tillgång till patientens journal efter dennes begäran. Särskilda rutiner/regler finns för hur personalen ska gå tillväga i sådana fall.

4/ Utlämnande av journalinformation: uppfyllt men med kvarstående otydligheter

TC ger möjlighet att göra utskrifter till patienter efter begäran. Utlämnande kan ske efter sedvanlig menprövning till berörd patient. En användare d.v.s. i detta fall en informationsägare (verksamhetschef) får dock endast lämna ut information som tillhör dennes verksamhet. I en sammanhållen journal finns information från flera verksamheter samlad på samma ställe vilket är själva syftet. Vid en utlämnandesituation kan detta dock medföra komplikationer så till vida att det kan vara svårt för användaren att inse vilken information som får respektive inte får lämnas ut. Även om TC i viss utsträckning indikerar vem som är ägare till informationen så är denna markering idag inte tillräckligt tydlig för att misstag ska kunna undvikas.

5/ Loggning: delvis uppfyllt

I TC registreras (loggas) transaktioner om vem som har öppnat en journal och när. Två typer av granskning av dessa loggar sker. Den ena är att det varje gång en journal öppnas för en viss patient visas en meny med uppgifter om dem som de senaste 10 gångerna öppnat journalen. De uppgifter som visas är från vilken vårdenhet användaren öppnade journalen och tidpunkten för detta samt befattning. Detta ger en möjlighet för den som har patientkontakt att vid varje ny öppning bedöma om uppvisade inloggningar är rimliga eller om de ska rapporteras för vidare granskning. Det andra är en månadsvis slumpmässig selektion av öppningar av ett antal patientjournaler för vilka det visas vilka användare som öppnat dessa. Ett bestämt antal öppningar väljs ut per vårdenhet för alla organisationer som ingår i Karolinskas installation. Resultatet skickas till respektive informationsägare per vårdenhet för granskning. Finner denne någon journalöppning som inte förefaller korrekt ska kontakt tas med vederbörande för ett klagande. Kvarstår oklarheter kan detta bli ett personalärende angående dataintrång.

Datainspektionen har i ett tillsynsbeslut (dnr 761-2008) enligt Personuppgiftslagen (1998:204) från april 2009 avseende Karolinska framfört kritik mot bristande loggningsrutiner. KU har i maj 2009 i en åtgärdsplan redogjort för de tre steg som skulle vidtas till följd av kritiken. I/ Under juli respektive oktober 2009 ökades stickprovsstorleken för loggningen. II/ Under januari 2010 infördes, tre månader försenat, en effektivare stickprovsmetod. III/ Under 2010 ska ett sk intelligent logganalysystem, som nu är under utveckling, införas. Enligt tillsynsbeslutet har Datainspektionen för avsikt att följa upp ärendet. Styrelsen för Karolinska har i enlighet med Datainspektionens tillsynsbeslut lämnat en lägesbeskrivning senast den 1 februari 2010. Datainspektionen handlägger för närvarande ärendet (ärendenr 217-2010).

6/ Aktiva val: delvis uppfyllt

Enligt Socialstyrelsens föreskrifter till Patientdatalagen krävs att användaren, i vissa situationer, för att få ta del av uppgifter först gör en bedömning och sedan som en bekräftelse gör ett aktivt val i systemet. Det aktiva valet ska loggas. I TC finns funktioner för sådana aktiva val vad gäller journaltext.

Däremot finns det i TC inte aktiva val för andra dokument såsom t.ex. Blodprovssvar, LM-journal, Röntgenundersökningar, Konsultremisser och Diagnoser. Således uppfylls inte kraven i Patientdatalagen avseende dessa sistnämnda dokument. För att åtgärda detta har en aktivitet startats inom CSTC där utvecklingsgruppen och leverantören går igenom och gör en riskanalys för alla typer av dokument. Därefter fattas beslut om det ska införas aktiva val för dem under 2010.

7/ Spärrning: delvis uppfyllt

Enligt Patientdatalagen ska all medicinsk information kunna spärras av patienten. När Lagen trädde i kraft 2008-07-01, utan övergångsbestämmelser, fanns det inga spärrmöjligheter i TC. Förhållandet var detsamma för flertalet andra journalsystem.

Spärrmöjlighet av journalinformation genomfördes i TC den 2 juni 2009, dock med vissa undantag. Undantaget gäller vissa informationsmängder som bedömts vara särskilt känsliga och därför inte lämpliga att ge patienten spärrmöjlighet för. Vid tolkningen av Patientdatalagen och avvägningen mot patientsäkerheten gjordes tidigt bedömningen av Policygruppen (chefsläkare) att det fanns ett visst tolkningsutrymme, så att information som var särskilt viktig för; patienten, andra patienter och personalen, skulle kunna undantas från spärrmöjligheten. Vårdgivarnas representanter, Policygruppen knuten till CSTC beslutade sålunda enligt minnesanteckningar 2009-02-20 att av patientsäkerhetsskäl exkludera informationen i "Läkemedelsmodulen" (LM) och "Viktig Medicinsk Information" (VMI) från spärrmöjligheten i första fasen av införande.

I applikationen har emellertid leverantören skapat en funktion som möjliggör sådan spärrning i Läkemedelsmodulen dock, först efter det att leverantören aktiverat funktionen. Någon sådan aktivering är ännu inte gjord. Efter grundläggande genomgång av förarbeten till Patientdatalagen där invändningar kring patientsäkerheten behandlas ansågs alla invändningar ha tagits hänsyn till och att dessa sammantaget inte överväger patientens behov av integritet i form av rätten till spärrning. Därefter har diskussionen förts vidare i Policygruppen. Denna har efter interna diskussioner under hösten 2009 kommit fram till, att trots invändningarna kring patientsäkerheten, ska möjligheten till spärrning införas. Leverantören avser därför den 9 februari 2010 att leverera spärrmöjligheten till applikationen. Innan den aktiveras ska leverantören genomföra och presentera en riskanalys för Policygruppen den 19 februari. Gruppen avser att i samband med detta tillfälle överväga huruvida en aktivering ska ske av spärrning för Läkemedelsmodulen.

För Viktig medicinsk information finns ingen spärrningsfunktion framtagen ännu. Därför kommer det att dröja ytterligare en tid innan en sådan kan aktiveras. Enligt en bedömning av systemägaren kan det ta en dryg månad för leverantören att konstruera en sådan funktion.

Konstateras kan att karolinskas installation idag inte har spärrmöjlighet i dessa båda avseenden och därmed inte uppfyller Patientdatalagen. Att skapa sådana funktioner

inom TC kan enligt uppgift från systemägaren ske med relativt kort varsel. Det är emellertid inte i första hand ett systemmässigt problem utan snarare ett verksamhetsmässigt problem där intrikata riskbedömningar mellan patientsäkerhet och patientintegritet ställs på sin spets. Genom att utveckla spärrfunktionerna för både Läkemedelsmodulen och Viktig medicinsk information uppfyller applikationen TC och därmed leverantören Patientdatalagens krav. Är dessa funktioner sedan inte aktiverade är det inte leverantörens ansvar. Ansvaret vilar då snarare på vårdgivarna och deras representanter i STC som inte beslutat att ge systemägaren i uppgift att låta aktivera spärrmöjligheterna.

8/ Kryptering: ej uppfyllt

Socialstyrelsens föreskrifter till Patientdatalagen anger att information som skickas över öppna nät ska vara krypterad. Information i TC skickas via landstingets gemensamma IT-nät SLL-net vilket betraktas som ett öppet nät. Men det finns idag ingen funktion för kryptering av information i TC. Två lösningar förespråkas som båda sägs vara klara för installation vid halvårsskiftet 2010. Huvudalternativet är kryptering i SLL-ITs för hela SLL gemensamma plattform. Andrahandsalternativet är leverantörens lösning genom uppgradering av TC till ny version av applikationens systemprogramvara APL (version 12).

9/ Stark autentisering: ej uppfyllt

Socialstyrelsen föreskrifter till Patientdatalagen innehåller krav på att identifiering för en sammanhållen journal ska ske med två komponenter t ex kort och kod. Detta kan idag inte ske i TC. Förutsättningar för en sådan stark autentisering bedöms dock komma att finnas när den för SLL gemensamma IT-plattformen införs. Det införandet bedöms komma att ske vid halvårsskiftet 2010.

Analys

När Patientdatalagen infördes 2008-07-01 var situationen den att inga journalsystem och ej heller TC fullt ut uppfyllde de krav som lagen ställde. Det var också så att det inte alltid fanns några självklara systemmässiga och tekniska lösningar som enkelt kunde införas. Lagen ägde sin giltighet medan journalsystemen trots sina legala brister fortsatte att vara i drift.

Systemägaren har inom ramen för CSTCs verksamhet liksom Policygruppen (chefsläkare) bedrivit ett omfattande arbete med att analysera och bedöma vad lagstiftningen innebär, inte minst för en sammanhållen journalföring och hur dessa frågor ska hanteras i TC. Sedan lagen infördes har ett antal åtgärder vidtagits för att nå upp till lagens intentioner. Detta har dock ännu inte lyckats till fullo.

Det pågår arbete med inriktningen att helt uppfylla lagens krav. Komplexiteten i att skapa sammanhållen journalföring och leva upp till lagens krav i ett befintligt system i drift samtidigt som patientsäkerheten upprätthålls ska inte underskattas. Därtill kommer att TC ska anpassas till IT-strategi och IT-miljö inom SLL.

Genomgången av nio viktiga krav på förändringar som lagstiftningen inneburit för TC visar att fyra är uppfyllda, tre är delvis uppfyllda och två är inte uppfyllda.

Konstateras kan att TC efter drygt ett och ett halvt år fortfarande till vissa delar inte uppfyller Patientdatalagen.

3.3 Har analys gjorts av om TakeCare är i linje med den nationella IT-strategin för vård och omsorg?

Iakttagelser

Den Nationella IT-strategin för vård och omsorg som publicerades i mars 2006 är framtagen i ett samarbete mellan Socialdepartementet, Sveriges kommuner och landsting, Socialstyrelsen, Läkemedelsverket, Apoteket AB och Carelink. Grundidén är att patientsäkerhet, vårdkvalitet och tillgänglighet inom vård och omsorg kan kraftigt förbättras genom användning av olika former av IT-stöd. I strategin konstateras att en rad frågor av betydelse för IT-användningen måste lösas på nationell nivå i samverkan mellan alla aktörer inom vården.

I strategin pekas sex insatsområden ut. De är:

1. Harmoniera lagar och regelverk med en ökad IT-användning
2. Skapa en gemensam informationsstruktur.
3. Skapa en gemensam teknisk infrastruktur
4. Skapa förutsättningar för samverkande och verksamhetsstödjande IT-system.
5. Möjliggöra åtkomst till information över organisationsstrukturer
6. Göra information och tjänster lättillgängliga för medborgare.

Huvuddelen av arbetet med att effektivisera vården måste utföras av de enskilda landstingen, kommunerna och privata vårdgivarna. Men i strategin konstateras också att varje landsting och kommun beslutar själv i kraft av det kommunala självstyret för vilka ändamål och på vilka sätt IT ska användas samt upphandlar och utvecklar de IT-stöd de beslutar om.

Alla landsting har beslutat att anta den nationella IT-strategin och har tagit en gemensam handlingsplan för att förverkliga den. SLL har enligt lägesrapport 2009 angående den nationella IT-strategin implementerat eller har avtal om införande av samtliga förvaltningsprojekt inom ramen för samarbetet.

Arbetet på nationell nivå har till stor del bestått i att verka för att gemensamma nationella normer tas fram. Arbetet med normerna har pågått under flera år och först under slutet av år 2009 presenterades ”standarderna” för den nationella informationsinfrastrukturen. På motsvarande sätt har det varit vad gäller den nationella patientöversikten som sedan en tid varit i provdrift i ett landsting. De mer närliggande frågorna för CSTC har dock varit att ta ansvar för, utveckla och förvalta TC för vården inom SLL i väntan på att normer och standards färdigställs. Först när sådana finns är det möjligt för CSTC att förhålla sig till hur de bör påverka TC.

För att ytterligare stärka SLLs funktion med att både påverka och återföra information från den nationella nivån inrättades 2008 en tjänst inom Landstingsstyrelsens förvaltning som central koncernsamordnare-IT. Genom detta finns en representant för SLL i det gemensamma nationella arbetet och en länk till verksamheten inom SLL. Exempelvis är innehavaren av denna tjänst adjungerad till styrelsemöten i STC. En kanal finns därmed för att kunna föra intentioner och kompetens från det nationella samarbetet vidare till CSTC.

Inom CSTC verkar man i den riktning som strategin visar om än på en mer systemnära samt vård- och verksamhetsnära nivå. TC ska nu som resultat av sitt tidigare nationella samarbete börja leverera information till den nationella patientöversikten. Genom att TC möjliggör en sammanhållen journalföring blir de insatsområden som anges i strategin viktiga för funktionen av systemet.

Analys

Någon analys av om TC ligger i linje med den nationella IT-strategin för vård och omsorg som resulterat i ett enhetligt dokument har systemägaren inte tagit fram.

Arbetet med att skapa TC för en sammanhållen journalföring är emellertid i sina huvuddrag i linje med den nationella IT-strategin. Att utvecklingen går i riktning mot de sex insatsområdena beror dels på den nationella samverkan, dels på rationella krav avseende effektiv verksamhet och resursanvändning.

3.4 Har analys gjorts av om TakeCare är långsiktigt funktionellt?

Iakttagelser

TC har varit i drift under lång tid för Huddinge sjukhus och sedan för Karolinska. Antalet vårdgivare och användare har successivt utökats. Förvaltningsorganisationen har utvecklats under tiden. Under de senaste åren har en central förvaltningsorganisation skapats genom inrättandet av STC och CSTC. Inom ramen för STC och CSTC har det förts och förs diskussion om hur TC ska stärkas för att vara långsiktigt funktionellt. Denna diskussion förs bl.a. med verksamhetsrepresentanter, leverantören och SLL-IT. Ett samarbete enligt den nationella IT-strategin sker med andra landstingsexterna parter. Tydligare rollbeskrivningar har tagits fram och avtal slutits mellan medverkande parter i STC liksom mellan CSTC och leverantörer. Syftet med denna organisation är att skapa en styrfunktion för TC som verkar för ett långsiktigt funktionellt TC.

Begreppet långsiktigt funktionellt innebär att systemet förväntas vara väl fungerande för verksamheten under överskådlig tid. Hur lång tid det rör sig om för ett system med den spridning till olika vårdgivare som TC går inte att slå fast. Men att det torde röra sig om 5-10 år är en rimlig uppskattning. Långsiktigt funktionellt kan också skildras ur olika aspekter. Några av de mest väsentliga beskrivs nedan.

1/ Sammanhållen journalföring

Grunden för TC är journalföring och för långsiktigheten är målen i den nationella strategin väsentliga rättesnören. TC verkar genom uppbyggnaden av den sammanhållna journalföringen i enlighet med dessa mål. Själva egenskapen sammanhållen journalföring är emellertid inte specifik för TC utan finns även i andra leverantörers produkter. Men genom att innehålla denna funktion medför TC en effektivisering av arbetet inom vårdsektorn i riktning mot "en patient en journal" och är ur den aspekten långsiktigt funktionellt.

2/ Verksamhetsmässigt

Utvecklingsstrategin för TC innebär att bygga systemet på erfarenheter från och i nära samarbete med verksamheten d.v.s. representanter för vården. Detta betraktas vara en framgångsfaktor för att uppnå god funktionalitet och en förankring i hur arbetet i praktiken ska garanteras stöd av TC. De personer som intervjuats under granskningen framhåller, även om de har synpunkter på förbättringar, TCs styrka som verksamhetsmässigt funktionellt.

3/ Användarvänlighet

Grundtanken med TC är att det ska byggas utifrån ett användarperspektiv för att bli effektivt i verksamheten. De användare som intervjuats under denna uppföljning ger också en positiv bild av TC. I en särskild aktivitet lät Profdoc Care AB under 2005 TC genomgå en process för användarcertifiering. Detta resulterade i att TC då blev det första journalsystemet som användarcertifierades (se www.useraward.se).

4/ Tekniskt

TC bygger på systemprogramvaran APL. Det har vid några tillfällen bl.a. i media framförts kritik mot nyttjandet av APL mot bakgrund att ursprungsversionen av detsamma är utvecklat 60-talet och har relativt få användare. Förvisso har APL använts under lång tid men det har som de flesta andra programspråk uppgraderats i flera versioner. Ålder på en ursprungsversion behöver således inte vara något relevant kriterium för att framföra kritik. Det som bör avgöra om APL är tekniskt funktionellt är snarare om dess struktur passar för de tillämpningar som är dominerande i TC. Under uppföljningen är en framträdande uppfattning att APL är lämpat för transaktionsintensiv verksamhet. Med det stora antal användare som dagligen nyttjar TC, det stora antalet journalöppningar och behovet av direktåtkomst torde egenskaperna i APL lämpa sig för TC behov.

Mängden applikationer som är skrivna i APL må relativt sett vara liten jämfört med de mest spridda språken. Men det finns fortfarande ett stort antal stora kunder internationellt som har betydande applikationer skrivna i APL och har krav på långsiktighet. Det gäller inte minst inom bank- och finanssektorn som har transaktionsintensiv verksamhet. Leverantören av APL tycks bedöma marknaden som tillräckligt stor för att fortsätta att utveckla produkten. Under första halvåret 2010 släpps en ny version, nr 12.

5/ Kompetens

För att en applikationsleverantör som Profdoc Care AB samt CSTC är det väsentligt att det går att hitta tillräckligt med kompetenta medarbetare som kan hantera APL. Detta har hittills fungerat väl. Dessutom anses APL vara relativt enkelt för en duktig programmerare att lära sig till en tillfredsställande nivå.

6/ Ekonomi

Finansieringen av TC sker genom en årsavgift för den gemensamma förvaltningen genom en avgift per årsanvändare av dem som nyttjar TC. Dessa bidrar också med kompetens till samverkansarbetet. Det är CSTC som sluter avtal med externa leverantörer.

Kostnaden för nyttjandet av TC i form av licens har avtalats bort med leverantören. Karolinska har tillgång till TC via ett avtal slutet för Huddinge sjukhus. Det omfattar sjukhusets organisation och inkluderar dotterbolag och vårdgivare med vilka man har samarbete samt sjukvården Gotland. Det ger en icke-exklusiv rätt och tidsobegränsad licens att nyttja TC giltigt för ett obegränsat antal användare och installationer. Detta avtal innebär således att Karolinska och de som är ingår i samverkansarbetet i STC regi inte betalar någon licenskostnad. Däremot ersätts leverantören för utveckling och underhåll som CTSC beställer. Ekonomiskt innebär detta att totalkostnaden att fördela blir lägre än annars. Det stora antalet användare till TC ger i sin tur en bred bas att fördela kostnaden på. Sammantaget ger detta vad som uppfattas som en låg kostnad per

användare. Flera har uppgivit att kostnaden per årsanvändare har gått ned markant sedan de bytt till TC.

Genom den sammanhållna journalföringen blir verksamheten dessutom effektivare då man får tillgång till mer information direkt, slipper väntetider, slipper remittera ett antal prover och får därmed lägre laboratoriekostnader. Ekonomiskt uppfattas TC vara långsiktigt funktionellt.

7/ Certifiering som medicinskteknisk produkt.

Lagen om medicintekniska produkter (SFS 1993:584) har omarbetats och ändringarna träder ikraft 2010-03-21. Bl.a. innebär detta att IT-baserade journalsystem klassas som medicintekniska produkter och ska uppfylla långtgående krav för att få släppas ut på marknaden. Det medför i praktiken att nya versioner av bl.a. journalsystem inte kan släppas ut på marknaden utan att ha genomgått en omfattande granskning (certifiering). Profdoc Care AB bedriver därför ett projekt för att TC ska uppfylla nämnda krav och uppnå en certifiering innan lagen träder ikraft. Syftet är att Profdoc Care AB ser TC som en strategisk produkt.

Analys

När det gäller frågan om systemägaren gjort någon analys av om TC är långsiktigt funktionellt så har ingen sådan genomförts som resulterat i ett enhetligt dokument. En sådan analys borde ha bestått av en beskrivning av såväl för- som nackdelar med TC och analysen hade kunnat vara underlag för hur resurser långsiktigt bäst skulle kunna prioriteras. Dokument skulle ha ökat transparensen kring TC och underlättat för berörda beslutsfattare att få en bild av tillståndet kring systemet och dess utvecklingsmöjligheter.

Avsaknaden av ett dokument med en samlad och långsiktig analys innebär emellertid inte per automatik att någon analys överhuvud taget inte har gjorts. De åtgärder som vidtagits visar på ett kontinuerligt arbete med att överväga lämpliga sätt för att säkra att TC blir långsiktigt funktionellt. En kontinuerlig diskussion inom CSTC, dess styrelse och grupper torde ligga till grund för detta arbete. En samlad analys hade emellertid ökat tydligheten och gett beslutsfattarna bättre möjlighet till avvägningar mellan olika handlingsvägar.

3.5 Har en säkerhetsgranskning genomförts?

Iakttagelser

Säkerhetsgranskningar har genomförts inom TC som separata aktiviteter. De aktiviteter som utförts eller pågår är:

1/ Systemägaren och förvaltningsorganisationen genomförde 2008 med bistånd av externa konsulter en riskanalys avseende TC. Denna var i huvudsak inriktad på risker kring systemutveckling, tester, processer, rutiner, policyer, driftstörningar, leverantörsrisker m.m. Den behandlade också risker kring informationssäkerhet och patientdatasekretess. Dess huvudsakliga fokus låg på åtkomstproblematiken hur risker kring skyddet av information skulle kunna elimineras med behörigheter, intrångsskydd i SLL-net samt förberedelsearbetet kring nya krav till följd av en ny patientdatalag.

I den riskanalysen lyfts problematiken kring administrativa rutiner, fysisk säkerhet och kryptering i viss mån fram. Den behandlas inte ingående i det riskanalysdokument som

upprättats men problemen tydliggörs och CSTC har tagit ställning till vart och ett av dem och adresserat dem till en mottagare vilken oftast är CSTC eller någon undergrupp knuten till densamma. De externa konsulterna har därefter tagit ställning till de identifierade riskerna och CSTCs bedömning.

2/ På grund av det haveri som inträffade i TC 2008-12-18 genomfördes en ingående säkerhetsgranskning avseende orsakerna till avbrottet under inledningen av 2009. Den avsåg främst drift- och återställningsfrågor men behandlade i viss mån också administrativa rutiner, fysisk säkerhet och kryptering. Rapporten som skrevs till följd av avbrottet beslutades av systemägaren utgöra den årliga säkerhetsgranskningen för 2009. Granskningen ledde till att en särskild säkerhetsaktivitet skapades, det s.k. 8-programmet.

3/ 8-programmet inrättades inom CSTC för perioden 2009 - 2010 med syfte att vidta åtgärder till följd av avbrottet. Programmet består av representanter för de tre parterna systemägaren, SLL-IT och leverantören. Programmet har tagit fram en handlingsplan och under 2009/2010 utfört ett omfattande arbete med att genomföra bl.a. de förslag som lämnats i haverirapporten. Programmet kommer att avslutas senast vid halvårsskiftet 2010. Systemägaren planerar att under 2010 genomföra en uppföljning av 8-programmet som en särskild säkerhetsgranskning. Denna sistnämnda aktivitet har dock ännu inte tagit någon konkret form vad avser projektplan, budget eller upphandlingsunderlag.

Socialstyrelsen har med anledning av avbrottet i TC 2008-12-18 initierat ett Lex Maria ärende (SoS dnr 41-115672009). Bl.a. påpekas att vårdgivarna inte följt Socialstyrelsens föreskrifter SOSFS 2008:14) om informationsbehandling och journalföring i hälso- och sjukvården där det finns krav på att återläsningsprov görs av säkerhetskopior. Därtill påpekades att den säkerhetsgranskning som initierades av CSTC visade på brister i kvalitetsledningssystemen vid händelsen. Krav på ledningssystem finns i Socialstyrelsens föreskrifter (SOSFS 2005:12) samt krav på informationshantering och journalföring i föreskrifterna (SOSFS 2008:14). CSTC har utarbetat en handlingsplan och rapporterat till Socialstyrelsen om pågående arbete med förbättring av driftsäkerheten i TC. Socialstyrelsen har enligt beslut 2009-12-15 för avsikt att följa upp ärendet under våren 2010.

Ett system så betydelsefullt för verksamheten och av den omfattningen som TC kräver emellertid att informationssäkerhetsarbetet ges mycket hög prioritet. En iakttagelse är att det saknas rutiner inom CSTC för när och hur säkerhetsgranskningar ska genomföras i verksamheten. Visserligen är CSTC formellt kopplad som en enhet till Karolinska och bör följa de rutiner som finns där. CSTC har emellertid i praktiken en så fristående ställning att det för tydlighetens skull är lämpligt att regler och rutiner fastläggs även för denna verksamhet.

Några initiativ till en framåtsyftande och förutsättningslös aktivitet för riskinventering har inte tagits sedan 2008. Det som gjorts har snarare varit styrt av omständigheterna och inriktat på att lösa visserligen viktiga, omfattande och komplexa problem men likafullt utgående från en händelse. Den pågående generella riskdiskussion som pågår sker inte samlat och det finns heller ingen tydlig redovisning, bortsett från 8-programmet, av densamma.

Analys

Säkerhetsgranskningar har initierats av den centrala förvaltningen för TC som en gemensam aktivitet för karolinskas installation, vilken samverkan inom STC avser. Det har dels skett i ett initialt skede 2008, dels på förekommen anledning efter avbrottet 2008-12-18.

Granskningarna har behandlat administrativa rutiner, fysiskt skydd och logiskt skydd om än i olika grad. De har också varit föremål för omfattande arbete inom CSTC, SLL- IT och leverantören. Utöver dessa särskilda säkerhetsgranskningar diskuteras säkerhetsfrågor kontinuerligt inom ramen för CSTC. Systemägaren har haft en tongivande roll i arbetet med att initiera säkerhetsgranskningarna.

Enligt uppföljningsfrågan krävs att ”systemägaren och respektive informationsägare genomför en riktad säkerhetsgranskning av redan befintliga installationer vad beträffar skyddet av information”. Systemägaren får anses ha genomfört en riktad säkerhetsgranskning och att omständigheterna lett till en större säkerhetsgenomgång samt att ett analysförfarande av informationssäkerheten har fortgått inom den ordinarie verksamheten. När det gäller informationsägarnas deltagande i riskanalyserandet så har det inte skett bokstavligt. En förklaring kan vara att granskningar genomförts på central nivå och en annan att det tidigare rått viss oklarhet om vem som är informationsägare i TC. Detta är dock inte acceptabla skäl för att avstå från att genomföra säkerhetsgranskningar. Sådana borde ha genomförts inom varje vårdenhet vad avser skyddet för information inom just den verksamheten. Om det för den enskilde informationsägaren var oklart vad som låg i dennes ansvar borde CSTC ha informerat dem om detta. Uppföljningsfrågan får med en strikt tolkning anses vara utförd för systemägarens del genom den aktivitet som gjordes 2008, medan den inte har utförts för informationsägarnas del.

Säkerhetsarbete utgör ett kontinuerligt arbete och det finns flera aktualiserade frågor kvar att lösa. Den säkerhetsgranskning som gjorts efter den första har varit knuten till den speciella händelsen, avbrottet 2008-12-18. Även om det också under 2009 gjorts en säkerhetsgranskning kan hanteringen inte anses vara tillfyllest eftersom det saknas en rutin för att årligen och oberoende av händelser genomföra granskningar. De ingår således inte i ett kontinuerligt säkerhetsarbete utan måste i ett processperspektiv betraktas som engångsföreteelser.

3.6 Har analys gjorts av hur SLL tillgodoser vårdens behov av journalsystem?

Iakttagelser

När granskningen gjordes 2007/2008 var förutsättningarna annorlunda än idag. Granskningen gjordes i ljuset av den mycket splittrade bild avseende journalföringssystem som länge varit gällande inom SLL. Då fanns 26 olika journalsystem vilka inte kommunicerade med varandra. Vid denna tidpunkt bedrevs också det stora projektet Gemensam VårdDokumentation som skulle lösa problemet och skapa datalagring och kommunikationsmöjlighet mellan systemen. Sedan dess har projektet lagts ned. Behovet av att få åtkomst till journalinformation mellan vårdenheter kvarstod dock liksom problemen med kommunikation mellan systemen.

SLL stod inför i princip två alternativ; det ena var att fortsätta försöken med att koppla samman befintliga system eller att införa ett enhetligt system. Det första var redan prövat men

hade visat sig vara förknippat med stora svårigheter. Det andra var heller inget självklart alternativ utan även det var förknippat med svårigheter. Följande faktorer kom starkt att påverka situationen:

1/ Vid skapandet av Karolinska i Solna/Huddinge beslutades att denna organisation skulle använda TC som journalsystem. Karolinska hade slutit ett avtal med leverantören utan några licenskostnader. Dessutom gav avtalet rätt att expandera användningen till ett obegränsat antal användare och installationer inom sjukhusets organisation vilket också innefattade dotterbolag samt andra vårdgivare man samarbetade med. Här fanns således incitament för andra att ansluta sig. Så skedde också och ett strategiskt viktigt steg var när SLSO beslöt sig för att ansluta sina verksamheter till TC. Därmed hade TC blivit det dominerande journalsystemet inom SLL.

2/ Under 2009 har därtill landstingsdirektörens uttalande att TC ska utgöra huvudalternativet för valet av journalsystem inom SLL, starkt påverkat utvecklingen.

Det gjorde att ett alternativ mellan de båda ovan angivna har utvecklats. TC har vuxit ytterligare i volym och är stadd i fortsatt expansion. Till dags dato är många vårdgivare anslutna och TC har 25 000 användare samt en databas med uppgifter om 2,2 miljoner patienter. TC är det dominerande journalsystemet men det finns flera andra journalsystem i drift inom SLL bland både offentliga och privata vårdgivare. Idag finns inget beslut om att knyta samman dessa eller kräva att samma system ska användas. Vårdgivarna får snarare finna den lösning som är bäst för den egna verksamheten.

Under uppföljningen har de som intervjuats framfört i stort sett en i grunden samstämmig positiv bild om TC. Men det har också framförts kritik på enskildheter samt många synpunkter på förbättringar och kompletteringar. De intervjuade har emellertid inte ställts inför att väga för- och nackdelar avseende TC jämfört med något alternativt journalsystem.

En positiv faktor för TC är emellertid att man uppfattar det vara utvecklat från en verksamhetsnära utgångspunkt. I övrigt så förefaller det vara funktionen sammanhållen journalföring som är den avgörande faktorn för den positiva inställningen. Denna är systemoberoende men det är i TC som de intervjuade först möter denna funktion. Därmed ligger det i sakens natur att den positiva egenskapen kommer att tillskrivas TC även om andra system numer är likartade på denna punkt.

Analys

Någon förutsättningslös analys av hur Stockholms läns landsting bäst skulle tillgodose vårdens behov av journalsystem finns inte dokumenterad från tiden efter granskningen. Det innebär dock inte att denna fråga inte diskuterats och olika alternativ prövats.

Den utveckling som lett fram till dagens situation har emellertid inte grundats på resultatet av en i efterhand identifierbar analys utan snarare på ett antal beslut och omständigheter som i olika grad bidragit till att förhållandena idag ser ut som de gör. På frågan om hur Stockholms läns landsting bäst tillgodoser vårdens behov av journalsystem finns det därför inte något tydligt svar.

Trots avsaknad av regelrätt analys liksom en ingående funktionell jämförelse mellan olika journalsystem förefaller den uppfattning som flertalet av de intervjuade förfäktar vara att TC, inkluderande synpunkter på detsamma, tillgodoser vårdens behov av journalsystem.

Utveckling pågår därtill kontinuerligt för att anpassa och förbättra systemet.

3.7 Har analys gjorts av om åtgärder är i linje med SLLs IT-strategi?

Iakttagelser

När granskningen gjordes var en ny IT-strategi för perioden 2008-2013 under utarbetande. Den antogs 2008-04-21 av landstingsdirektören och har sedan förankrats hos förvaltningscheferna.

Strategin innehåller beskrivningar av både mål och strategisk inriktning, specificerade i ett antal punkter. IT-strategin bygger på att det finns en gemensam infrastruktur kring styrning och beslut samt IT-verksamhetsinriktning. Att medverka till att mål och inriktning följs är ett ansvar som ligger på TC. Det är emellertid också flera andra parter som har ett ansvar i detta samspel. För att helt följa strategin är CSTC också i vissa avseenden beroende av dessa parter ansvarstagande avseende koncerngemensamt IT-stöd för exempelvis kryptering i SLL-net och stark autentisering.

Det finns dock en punkt där TC inte fullt ut följer de mål som satts upp. Det gäller *”tillgängliggörandet av lagrad information rörande enskilda patienter inom ramen för lagar och förordningar som reglerar hälso- och sjukvården”*. Som beskrivits i avsnitt ovan finns det fortfarande problem med att TC inte uppfyller Patientdatalagen fullt ut i detta avseende. Arbete med att åtgärda dessa brister pågår dock.

Under den strategiska inriktningen anges också att *”förvaltning ska bedrivas enligt i SLL fastställd förvaltningsmodell”*. Det förvaltningsobjekt som CSTC ansvarar för är en samverkan avseende ett för flera vårdgivare gemensamt system men med ansvarsmässigt åtskilda informationsmängder. Bl.a. detta gör att det i nu gällande IT-förvaltningsmodell (ver 1.5) inte finns någon tydlig form för hur CSTCs arbete bör bedrivas. Däremot finns det i IT-förvaltningsmodellen mycket annat som är tillämpligt för och därför bör följas även av CSTC. En fullständig genomgång av överensstämelsen mellan nuvarande förvaltning i CSTC och IT-förvaltningsmodellen har inte varit möjlig inom ramen för denna uppföljning. En sådan hade därtill inom kort kommit att bli inaktuell när det enligt uppgift f.n. pågår en revidering av IT-förvaltningsmodellen. En ny sådan beräknas kunna träda ikraft under året. När så skett bör en genomlysning göras av CSTC i syfte att organisation, roller, rutiner etc så långt möjligt ska följa den nya IT-förvaltningsmodellen.

Analys

Någon förutsättningslös analys av om planerade och vidtagna åtgärder är i linje med IT-strategin finns inte dokumenterad från tiden efter granskningen. En övergripande genomgång av CSTCs agerande visar att detta i huvudsak följer strategins intentioner.

3.8 Är CSTCs funktion för informationssäkerhet ändamålsenlig?

Iakttagelser

Ansvar för informationssäkerhet är enligt SLLs riktlinjer för informationssäkerhet fördelat på flera roller. Informationsägaren har ansvar bl a för att riskanalyser genomförs och att de samordnas med andra informationsägare. Systemägaren har bl.a. ansvar för att specificera skyddsnivån genom instruktioner, vidta åtgärder utifrån riskanalyser m.m. En informationssäkerhetssamordnare ska finnas för respektive förvaltning och bolag, d.v.s. i det här fallet på Karolinska.

För effektiviteten inom CSTC medför denna rollfördelning vissa konsekvenser. Det finns ett stort antal vårdenheter och därmed informationsägare för TC. Enligt uppgift är de över 200 stycken. Dessa finns hos flera olika vårdgivare och representerar såväl slutenvård som primärvård. Någon central representant för informationsägarna finns inte. Nämnda informationsägare har till ansvar att genomföra och samordna riskanalyser i ett starkt centraliserat system. Det är en svår uppgift och hittills har något sådant inte skett. Systemägaren har att ta hand om de resultat som kommer från riskanalyserna liksom ett stort antal andra uppgifter.

Någon informationssäkerhetssamordnare finns inte explicit för TC. Den funktion för denna arbetsuppgift som ligger närmast till hands är, genom den organisatoriska knytningen av CSTC till Karolinska, informationssäkerhetssamordnaren där. Denne har bl.a. att koordinera arbetet med incidenthantering och riskanalyser. Informationssäkerhetssamordnaren ska rapportera direkt till förvaltningschefen (sjukhusdirektören) och vara kontaktperson till landstingets informationssäkerhetschef. Någon motsvarande utpekad koppling till system- eller informationsägare finns inte.

Även om rollerna formellt existerar så tycks det vara svårt för innehavarna att samverka. Inte minst därför att informationsägarskapet är uppdelat på ett stort antal personer. Den modell som ligger till grund för riktlinjernas rollfördelning är inte optimal för en sammanhållen journalföring. CSTCs trots allt relativt sett fristående ställning från Karolinska kan också förorsaka att relationen till informationssäkerhetssamordnaren blir mer skir. Det kan också ifrågasättas om inte informationssäkerhetssamordnare vid andra förvaltningar/bolag borde ha mer formella relationer till CSTC.

Under denna uppföljning har också signaler framkommit om att det för såväl leverantören som SLL-IT i vissa fall skulle kunna möjliggöra stärkt samverkan om det fanns en tydligare motpart för generella informationssäkerhetsfrågor inom CSTC.

Under det senaste året har starkt fokus riktats mot att vidta åtgärder som förebygger att avbrott likt det i december 2008 ska inträffa igen. Detta har skett i 8-programmet där även andra säkerhetsfrågor har behandlats i viss mån. 8-programmet kommer emellertid att avslutas senast vid halvårsskiftet 2010. De åtgärder som där vidtagits har successivt implementerats för TC. När 8-programmet avslutas under 2010 kommer det, åtminstone som det nu ser ut, inte längre att finnas någon tydlig mottagare inom CSTC för tillkommande informationssäkerhetsfrågor.

En bidragande orsak till informationssäkerhetsarbetet inte antagit formen av en kontinuerlig process kan vara att det utöver de centrala riktlinjerna inte finns något explicit regelverk anpassat för just TC i form av instruktioner. Det finns regler avseende informationssäkerhet för olika delar av verksamheten men inte i en sammanhållen form. Det kan också vara en förklaring till att det saknas en sammanhållen och regelbunden redovisning av statusläget för informationssäkerhet. Statusredovisningar har dock skett för de delar som innefattas i 8-programmet.

I avsnittet om genomförd säkerhetsgranskning ovan konstateras att det under senare tid inte har gjorts någon framåtsyftande och förutsättningslös aktivitet för riskinventering samt att saknas rutiner inom CSTC för när och hur säkerhetsgranskningar ska genomföras i verksamheten.

Socialstyrelsen har i föreskriften SOSFS 2005:12 om ledningssystem för kvalitet och patientsäkerhet i hälso- och sjukvården bl.a. tagit upp riskhantering. I föreskriften SOSFS 2008:14 om informationshantering och journalföring anges att varje vårdgivare ska utse en eller flera personer för att ansvara för informationssäkerhetsarbetet. Så har också gjorts hos vårdgivarna men det finns ingen tydlig koppling för dem till CSTC.

Det är inte osannolikt att en del av problembilden som beskrivs ovan är en konsekvens av att rollerna och det till dem kopplade ansvaret är svårt att anpassa till den komplexa organisation som krävs till följd av den sammanhållna journalföringen.

Problemet som här föreligger är att det saknas en väl fungerande och tydlig funktion för informationssäkerhet.

Den organisation och ansvarsfördelning som finns kring TC i övrigt är inte enkelt överblickbar. Innebörden av roller och ansvar mellan de av parterna slutna avtalen, SLLs IT-förvaltningsmodell och SLLs riktlinjer för informationssäkerhet ger inte en helt otvetydig bild.

Analys

Organisationsformen för CSTC har skapats för att ta tillvara hanteringen av många intressenter kring kärnan, den sammanhållna journalföringen. SLLs styrdokument såsom IT-säkerhetsriktlinjer och IT-förvaltningsmodell innehåller inte helt anpassade strukturer för sammanhållen journalföring. Mot den bakgrunden är det upp till systemägaren att tillsvidare vidta lämpliga åtgärder i den egna systemförvaltningen för att organisera informationssäkerhetsarbetet och förbättra informationssäkerhetssamordnarnas och informationsägarnas kontaktytor i dessa frågor. I det här fallet kan det vara att inom CSTC inrätta en separat sammanhållande funktion för informationssäkerhet trots att en sådan inte finns anbefalld i SLLs centrala regelverk.

En invändning skulle kunna vara att det inte behövs en särskild funktion för detta inom ett specifikt system, enär det redan finns ansvar utdelat för dessa uppgifter enligt regelverket. Utöver att det finns vissa otydligheter i nuvarande situation och att konsekvensen tycks vara uteblivet säkerhetsarbete så påverkar CSTC agerande en mycket stor, vittförgrenad och viktig verksamhet. Detta talar i sig för att informationssäkerhet bör lyftas fram som organisatorisk funktion.

Kopplingen mellan de berörda vårdgivarnas ledningssystem för kvalitet, enligt socialstyrelsens föreskrifter, och informationssäkerhetsarbetet i TC är inte tydlig. Kontaktytorna mellan ett system för sammanhållen journalföring och vårdgivarna blir naturligen många och kräver fastlagda och väl fungerande rutiner.

Sammantaget har CSTC arbetat med informationssäkerhet och vidtagit många viktiga åtgärder. Informationssäkerhetsarbetet är dock inte optimalt i den meningen att det inte har någon fast form och tydliga rutiner att följa. Konsekvensen kan bli att vissa risker inte belyses. Det saknas för att säkerställa ett kontinuerligt säkerhetsarbete såväl en tydlig funktion som väl beskrivna rutiner för informationssäkerhets- och riskhantering. Det föreligger också en otydlighet kring TC organisation och ansvarsfördelning som kan ge upphov till frågor och missförstånd.