YTTRANDE

Rasmus Havmöller
Rasmus.Havmoller@skane.se

Datum 2021-02-04
Ärendenummer 2021-POL000041

Redovisning till IVO avseende begäran om information inom ramen för tillsynsärende (IVOs dnr 3.5.1-00140/2021)

Inspektionen för vård och omsorg (IVO) har inom ramen för ett tillsynsärende (IVOs diarienummer 3.5.1-00140/2021, Region Skånes diarienummer 2021-O000045) inkommit med begäran om information.

Av begäran framkommer att den sker enligt 24§ Lag (2018: 1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

Tillsynen avser enligt begäran hur arbetet med riskanalys och riskvärdering skett inför och i samband med implementering av Region Skånes nya journalsystem. Begäran avser svar på fyra frågeställningar som redovisas och besvaras nedan.

Bakgrund

SDV (Skånes digitala vårdsystem) är ett uppkopplat vårdinformationssystem för bättre kvalitet och resultat i hälso- och sjukvården. SDV-systemet knyter samman hälso- och sjukvården i hela Skåne med gemensamma arbetssätt och består av tre huvuddelar;

- *Millennium:* ett nytt journalsystem som ersätter de olika separata system som idag används
- *CareAware:* ett system för infrastruktur och uppkopplad utrustning som bla ska ge möjlighet till kvalificerad vård i hemmet för patienter med kroniska sjukdomar
- *HealththeIntent (HI):* ett system som stärker det förebyggande arbetet med befolkningshälsan

Region Skåne har etablerat ett systematiskt och riskbaserat arbetssätt inom informations-säkerhetsområdet. Regionstyrelsen har beslutat om riktlinjer[1] som reglerar hur arbetet med informationssäkerhet inklusive riskanalys inom området skall bedrivas (fastställda 2017-12-07, Dnr: 1604263). Riktlinjerna kompletteras av Instruktioner[2] för tillämpning av riktlinjerna som fastställts av regiondirektören (2020-05-22, Dnr: 1800025). Dessa styrande dokument ligger till grund för arbetet med informationssäkerhet inom SDV och SDV-projektet har etablerat en tydlig process som bygger på dessa riktlinjer.

Det är regionstyrelsens uppfattning att för att i en allt mer komplex hälso- och sjukvård fortsatt kunna leverera god och säker vård utgående från invånarnas behov och möjliggöra en omställning till nära vård krävs en ändamålsenlig digital vårdmiljö. Region Skånes SDV-projekt syftar till att leverera denna förutsättning för att kunna möta invånarnas behov och förväntningar på hälso- och sjukvården men självklart med bibehållen informationssäkerhet.

Behovet av ett uppkopplat och sammanhållet vårdinformationssystem i Region Skåne identifierades redan 2011. Sedan dess har kraven på ett system utifrån såväl patientsäkerhet som IT-säkerhet ökat ytterligare. För regionstyrelsen är det angeläget att SDV-projektet kan slutföras med säkrat informationssäkerhetsperspektiv och att regionens svar på IVOs frågor nedan understryker detta.

Svar på begärd information

Här följer IVOs frågor (kursiverat) med regionens svar nedan respektive fråga.

1. *Hur har Region Skåne arbetat med testdata vid test av SDV? Hur har testdata tagits fram och hur har denna använts?*

För SDV-systemets tre huvuddelar (Millennium, CareAware och HI) arbetar Region Skånes SDV-projekt med anpassningar inom tre huvudområden:

- Mjukvaruutveckling, som rör det nya systemets ramverk, eller källkod
- Konfiguration
- Innehåll

I det första fallet, dvs avseende ändringar i källkoden måste detta beställas från leverantören Cerner Sverige AB. Dessa ärenden kan vara av varierande karaktär och omfattning, från att Region Skåne vill att personnummer ska skrivas på ett visst sätt till att mjukvaran anpassas till gällande standarder eller lagstiftning.

[1] https://vardgivare.skane.se/siteassets/2.-patientadministration/journalhantering-och-registrering/informationssakerhet/riktlinjer_for_informationssakerhet_beslut171207.pdf
[2] https://vardgivare.skane.se/siteassets/2.-patientadministration/journalhantering-och-registrering/informationssakerhet/instruktion-for-tillampning-av-riktlinje-for-informationssakerhet.pdf

Det andra stora området, konfiguration, kräver inga beställningar utan detta kan regionen själv påverka. Det kan exempelvis avse vad som först visas när man öppnar journalen eller hur ett blodtryck ska kunna dokumenteras.

Det tredje huvudområdet, anpassning av innehåll, omfattar exempelvis användare och behörigheter.

För att bekräfta att arbetet har resulterat i önskat resultat används testdata inom dessa arbetsområden. HI-installationen kommer att innehålla data för Region Skånes patienter. Omfattningen av data som används vid Millennium migrering är mycket mer isolerad och mindre omfattande än för HI Onboarding vilket har inneburit att olika metoder för skapande av testdata har använts.

Den generella testningen av SDV har genomförts genom att ett antal testpatienter har skapats i systemet. För att undvika att skarpa personnummer skapats av misstag har 100 personnummer från Skatteverkets testdatabas använts varvid dessa skrivits in som fiktiva patienter. Personer från SDV Function arbetsströmmar har använt fiktiv testdata med klinisk relevans men utan koppling till riktiga patienter i syfte att testa Millenniums konfigurationer.

Vid testning av CareAware i SDV används maskingenererad fiktiv testdata från den testade medicintekniska utrustningen kopplade till ovan nämnda testpatienter.

I korthet har således all hittills överförd data för teständamål enbart utgjorts av fiktiv eller anonymiserad data som inte kan härledas till någon person.

Testdata för Millennium migrering

Millennium laddningstest har genomförts med testdata som har skapats utifrån Millenniums datamodell baserat på vilken typ av data som finns i källsystemen. Syftet är att säkerställa automatisk migrering av nödvändig klinisk data från dagens källsystem till SDV Millennium med bibehållen riktighet. Målbilden är att kunna överföra klinisk data från befintliga journalsystem i drift (PMO, PASIS, Melior & Obsterix) under utrullning av SDV till Region Skånes verksamheter.

Testladdningar som har genomförts har ej använt data från källsystemen utan utgjorts av fiktiv data i samma format som källsystemen med en skapad unik Patientdatabas-id per patient kopplad till fiktiv data med samma format och datatyp som i källsystemen. Fiktiv data har skapats för testning av migrering till Millenniums applikationer för Demografi (PASiS/PMO), Aktiva graviditeter, Tillväxtkurvan (Melior/PMO) och Vårdtillfälle. För att undvika att skarpa personnummer skapats av misstag har 100 personnummer från Skatteverkets testdatabas använts. Fiktiv data har skapats för att täcka hela kodverket och alla enheter (cm, kg).

Efter migrering till Millennium genomförs granskning av mottagen data direkt i Millenniums databas samt i Millenniums applikation för att säkerställa att datan blivit korrekt överförd från en struktur i ett källsystem till Millenniums användarmiljö. Personer från SDV Function arbetsströmmar har skapat testdatan för att kunna motsvara klinisk relevans.

Ytterligare testning av systemets felhantering har genomförts genom att skapa felaktigheter i testdata, dvs felaktigheter mot kodverket för data såsom språkkod som ej finns i systemen. Tomma fält har även genererats för att testa systemets felhantering.

För att verifiera stabilitet och prestanda vid större dataöverföringar har maskinellt producerad fiktiv testdata använts, genom att generera en stor överföringsfil på ca 1,5 miljoner poster. Denna fiktiva data saknar klinisk relevans.

Testdata för HealtheIntent Onboarding (HI)

Laddning av data till HI kommer att ske bla från Region Skånes vårdinformationssystem. Planen är att göra en grundladdning av HI från de nuvarande systemen (Melior, PMO, PASiS och Obstetrix) ochta systemet i drift med HI innan ersättaren till dessa system, Cerner Millennium rullas ut i samband med SDV utrullning 1.0.

De initiala tekniska testerna för laddning från källsystemen till HI utförs i en testmiljö som finns tillgänglig hos leverantören (installerad i Cerners privata testdomän i Storbritannien, Cerner testdomän). Dessa testladdningar handlar om att säkerställa att laddningarna sker på ett tekniskt korrekt sätt avseende prestanda och korrekthet. Däremot testas ingenting avseende datas användbarhet för kliniska ändamål då det kommer att genomföras i en senare fas inom den svenska domänen (Region Skånes svenska HI-testdomän).

Första fasen av testladdningar har skett med avidentifierad data, dvs data som inte kan härledas till någon verklig person. Syftet är att använda diagnoskoder, resultat och annan data som är identisk med data i källsystemen för att kunna genomföra en mappning mellan källsystemets format och HI datamodell och på så sätt skapa en maskinell mappning för HI Onboarding.

Som källa används de befintliga utdatalagren för Melior, PMO och PASiS. Dessa innehåller skarpa patientdata. För varje källa väljs en lämplig mängd data från en ändamålsenlig tidsperiod ut. För varje källa väljs slumpmässigt ett antal patienter ut och för samtliga patienter väljs samtliga poster från tabellerna för patienter med avseende på data för Diagnoser, Resultat, Allergier, Åtgärder, Vaccinering, Ordinationer och Vårdtillfällen. Personnummer ersätts av ett slumpmässigt valt personnummer ur en lista av testpersonnummer (som ingen riktig person har) från Skatteverket. Namnfält och adressfält sätts till en slumpgenererad textsträng. De sålunda avidentifierade posterna skrivs till en fil per tabell med information om Patienter, Diagnoser, Resultat, Allergier, Åtgärder, Vaccinering, Ordinationer och Vårdtillfällen med samtlig dessa data upplagda på 10 patienter. HI-systemet kräver att minst 10 patienter har kodad data för att användas vid maskinell mappning.

Filerna överförs till Cerner Testdomän för laddning, behandling och validering mot de överförda filerna. Cerners informatiker och tekniker har bearbetat datan för att skapa en maskinell mappningsmodell i HI. Den laddade testdatan kommer att sakna betydelse för kliniska ändamål men är tillräcklig för de tekniska laddningstester som planeras. Testning av den kliniska relevansen av data och HI-applikationerna planeras till en senare fas före utrullning 1.0. All testdata raderas efter fullbordad testning.

2. *Hur har Region Skåne organisatoriskt arbetat med riskanalys och riskvärdering i SDV projektet?*

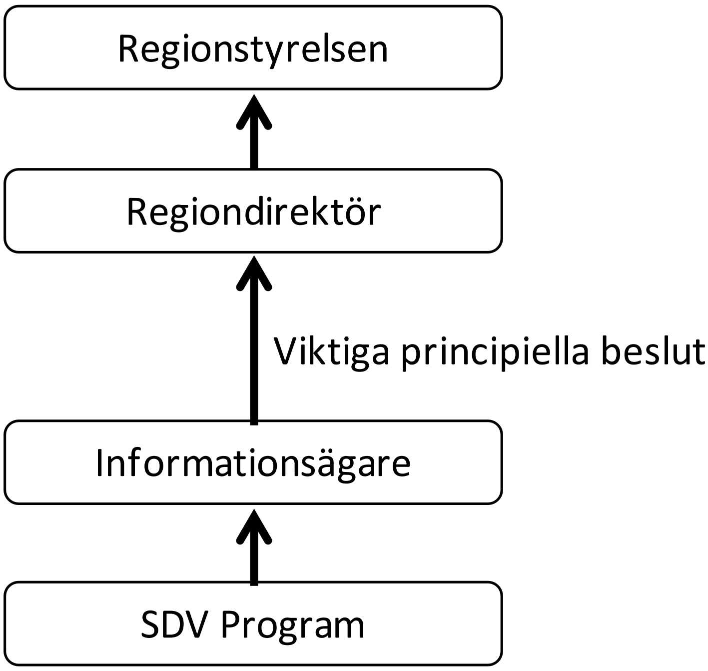
Region Skånes riktlinjer för informationssäkerhet ligger till grund för arbetet med informationssäkerhet inom SDV enligt följande principer:

- Inom SDV ska ett systematiskt informationssäkerhetsarbete bedrivas.

- Region Skånes informationstillgångar ska identifieras, klassificeras och ges en lämplig skyddsnivå.

- SDV ska, utifrån återkommande riskbedömningar och inträffade incidenter, avgöra hur risker ska hanteras och ge förslag på nödvändiga åtgärder för att upprätthålla rätt skyddsnivå för informationen.

- Fastställande av dessa bedömningar och åtgärder görs via Region Skånes normala beslutsprocess där informationsägare utgör primär beslutsfattare. Vid viktiga principiella beslut kan beslutsfattandet eskaleras till regionstyrelsen (figur 1).



Figur 1: Beslutsprocess SDV riskanalyser

SDV-projektet har etablerat en process som bygger på dessa riktlinjer där riskvärderingen utgår från programledningen. För att driva det praktiska riskanalysarbetet inom programmet har ett riskanalyskontor tillsatts som bla:

- identifierar områden där riskanalyser behöver genomföras och säkerställer framdrift samt bereder beslutsunderlag
- förbereder, faciliterar och dokumenterar riskanalyser
- överlämnar färdigställda riskanalyser till programmet för vidare hantering inom normal beslutsprocess

För att stödja riskanalyskontoret och i syfte att säkerställa att Region Skånes riktlinjer för informationssäkerhet följs har en gruppering (SDV Compliance) skapats inom SDV-programmet för att överse utvalda delar av riskanalysarbetet. Därvidlag har ett samarbete etablerats mellan projektresurser och expertfunktioner inom Region Skåne (juridik, dataskydd, informationssäkerhet, klinisk expertis och teknik). Respektive expertområde inom gruppen skall stödja SDV med identifiering och bedömning av risker samt dokumentera dessa inför beslut. Gruppen ska även identifiera eventuella behov av tillkommande områden och frågeställningar där riskanalyser behöver genomföras. För frågor med patientpåverkan involveras chefsläkare och chefssjuksköterska via den sk Clinical Risk Review Board.

Projektresurserna inom SDV Compliance har även representerat den kliniska sidan i det praktiska riskanalysarbetet.

3. *Vilka risk- och konsekvensanalyser har genomförts och vilka ställningstaganden har gjorts avseende överföring av patientuppgifter från befintliga system i test och produktion till det nya journalsystemet?*

Riskanalysarbetet har delats upp i enlighet med programmets övergripande systemkarta och styrs utifrån övergripande tidsplan. Avseende överföring av patientuppgifter från befintliga system är följande riskanalyser relevanta:

Genomförda riskanalyser i SDV-programmet:

- Förberedande aktiviteter inför driftsättning av SDV (Millennium Migrering och HI Onboarding av data)

Pågående riskanalyser i SDV-programmet:

- Huvudsystemen i SDV plattformen (Millennium, HI och CareAware)
- Stödsystem till SDV plattformen (t.ex. LightsOn och Taligenkänning)
- Anpassning av SDV avseende PDL

De genomförda riskanalyserna ”Förberedande aktiviteter inför driftsättning av SDV (Millennium Migrering och HI Onboarding av data)” fokuserar på riskerna kopplade till överföring av patientuppgifter från befintliga system till SDV och vilka behandlingar av patientuppgifter som finns kopplade till detta. Risker har analyserats utifrån följande område:

- Teknisk uppsättning
- Behandling av personuppgifter utifrån offentlighet- och sekretesslagen (OSL)
- Behandling av personuppgifter utifrån dataskyddsförordningen (DSF)
- Verksamhetsbaserade risker

De viktigaste ställningstaganden utifrån analyserna kan summeras enligt följande:

- Olika risker kopplade till den tekniska miljön inkl. hantering av cyberattacker har bedömts ligga mellan risknivå ”mycket låg” till ”medium” efter föreslagna mitigerande åtgärder. Verifiering av teknisk uppsättning föreslås ske genom en revision innan plattformen används inom vården.

- För att mitigera riskerna kopplade till OSL och DSF har begräsningar föreslagits kring vem som har access till personuppgifter. Detta gäller både för aktiviteter som behöver genomföras inom projektet och för supportfunktioner för den tekniska plattformen. Detta har lett till ett ställningstagande att all personal med access till personuppgifter skall vara fysiskt lokaliserade till Sverige och ha individuella uppdrag som osjälvständiga uppdragstagare till Region Skåne

- En analys specifikt kring risker kopplade till Cloud Act har genomförts och bedömts till en risknivå ”medium” för ett eventuellt utlämnande av personuppgifter vid inkommen begäran.

Då analyserna indikerar att inga risker kvarstår som har ett riskvärde på ”hög” eller ”mycket hög” efter mitigerande åtgärder finns det förutsättningar att gå vidare med planeringen för att överföra patientdata till SDV när åtgärderna genomförts och verifierats. Informationsägarens beslut att godkänna överföring av patientuppgifter har dock upphävts i avvaktan på ytterligare bedömning. En oberoende extern juridisk granskning genomförs. Hela ärendet skall därefter beredas på nytt och åter presenteras för informationsägare och regionstyrelsen för beslut i frågan.

4. *Vilka riskanalyser har genomförts och vilka ställningstaganden har gjorts gällande överföring av patientdata till tredje land? Vad är resultatet av dessa analyser?*

I riskanalyserna i samband med Migrering Millennium och HealtheIntent Onboarding (HI) har risker med överföring av personuppgifter till tredje land noterats. De noterade riskerna har resulterat i åtgärder i form av detaljerade instruktioner i Personuppgiftsbiträdesavtalet som begränsar all drift och support till resurser förlagda i Sverige under migreringsperioden. Vidare regleras att all personal som har åtkomst till personuppgifter i systemet antingen är anställda av Region Skåne eller har individuella uppdrag som osjälvständiga uppdragstagare till Region Skåne.

Vid regionstyrelsens sammanträde 2020-12-10 beslutades att migrering av data till Cerner inte ska genomföras förrän en oberoende granskning av de legala aspekterna rörande datahantering och datalagring inom ramen för SDV i relation till svensk och amerikansk (tredje lands) lagstiftning är genomförd. Även säkerhetspolisens synpunkter ska inhämtas som en del av utvärderingen.

Carl Johan Sonesson
Ordförande

Alf Jönsson
Regiondirektör