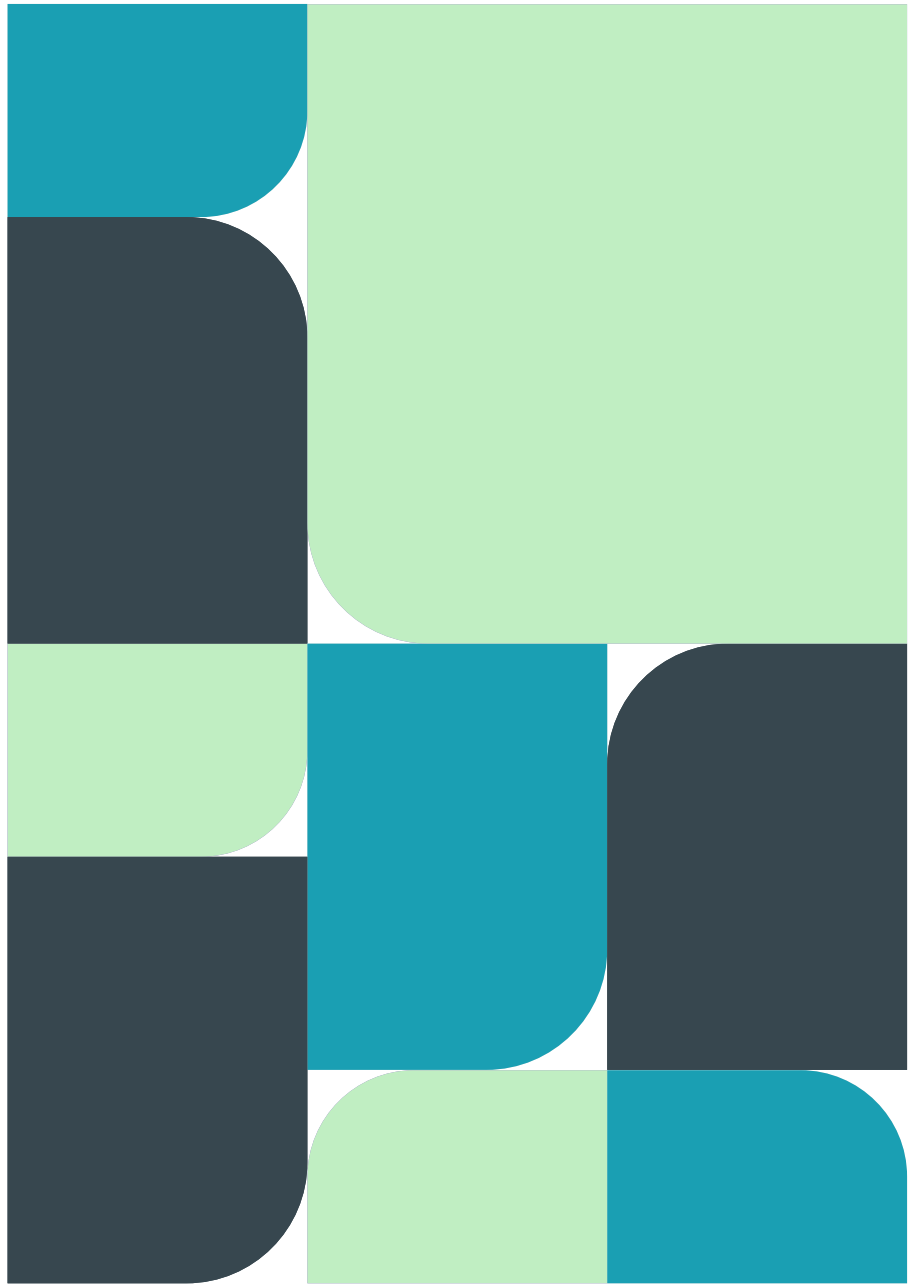
Vägval vårdinformationsmiljö, Informationssäkerhet

2025-02-26



VÄSTRA GÖTALANDSREGIONEN

Frågor

- Vad är det som utsätts för risk?
  - Information, personuppgifter, processer
  - Förtroende
  - applikation/mjukvara
  - Hårdvara
  - Människor
  - Rykte, image
- Hur påverkar alternativet informationens konfidentialitet?
  - Vilka hot är aktuella?
- Hur påverkar alternativet informationens riktighet?
  - Vilka hot är aktuella?
- Hur påverkar alternativet informationens tillgänglighet?
  - Vilka hot är aktuella?

1. Fortsätta med Cerner Millennium

- Nuvarande huvudsakliga version av Cerner Millennium implementeras
- Utrullning kommer sannolikt ske enligt annan utrullningsplan efter lessons learned efter PD1
- Implementeringen kan ha nuvarande, eller ett minskat scope
- Implementeringen sker on-prem men kommer på sikt att gå över till molndrift (Oracle OCI) och migreras till nästa generations Oracle EHR-system
- Exempel på alternativ framåt
  - Adressera funktioner som uppfattats som extra svåra och förbättra dessa:
    - Kan Oracle göra besvärlig funktionalitet enklare?
    - Är det möjligt att bryta ut komponenter som fungerat sämst och ersätta med bättre?
    - Går det att dölja kompexitet för användaren?
  - Lämna client hosted och gå in i modell som liknar Region Skåne
  - Låta visionen om den gemensamma vårdinformationsmiljön ta längre tid och börja införandet i någon utvald vårdverksamhet (slutenvård, primärvård, ….) för att sedan fortsätta bred utrullning längre fram

Risker - alternativ 1

- Risk att säkerhetsmekanismer inte fungerar eller missas p.g.a. den komplicerade ansvarsfördelningen mellan VGR och Oracle där ansvaret för säkerheten skiljer för olika delar av Millennium vilket utsätter informationen för risker.
- VGR förlorar viss kontrollen över informationen, svårt att försäkra oss om att informationen hanteras som vi tror eller som avtal säger.
- Risker kopplat till tillgänglighet (och kanske konfidentialitet) eftersom beroende till externa förbindelser (nätleverantörer) finns och blir allt mer centrala för åtkomst till OCI.
- Amerikanskt ägarskap i en alt mer osäker omvärld, risk för informationens konfidentialitet, risk kopplat till tillgänglighet om sanktioner eller tullar innebär för att vi inte får supportpersonal eller andra resurser för att säkra tillgängligheten. Scenario kan vara att amerikanska företag tvingas upphöra i EU.
- Risk att informationens riktighet påverkas omedvetet eftersom medarbetares inställning till Millennium gör att den utbildning som krävs inte går att genomföra.
- Millenniums komplexitet utgör risk för att mänskliga/organisatoriska oavsiktliga hot realiseras.
- Bristande förvaltning och/eller Oracles utveckling av Millennium eftersom fokus är på Oracle EHR innebär ökad risk för informationssäkerheten, exempelvis att systemens tillgänglighet försämras eller att sårbarheter inte åtgärdas i rimlig tid.
- Migrering i större omfattning innebär risk för informationens riktighet eftersom det krävs mycket tester som kan vara svårt att genomföra i förhållanden som liknar verkligheten.

2. Gå direkt mot nästa generations Oracle EHR-system

- VGR inväntar den nya version av Millennium som kallas Oracle EHR som annonserats under hösten 2024
- Innebär en molnbaserad (Oracle OCI) baserad lösning
- Fram till dess att Oracle EHR kan implementera måste befintliga eller nyanskaffade lösningar användas. Utgångspunkten är att Oracle EHR kan erbjuda viss funktionalitet senast 2027, sannolikt sker sedan tillägg av funktionalitet kommande år.
- Vi antar att vi fortsätter designa i Millennium och att Oracle tar fram verktyg att kunna migrera den designen till Oracle EHR enligt en uppgraderingsstrategi

Risker - alternativ 2

- VGR förlorar viss kontrollen över informationen, svårt att försäkra oss om att informationen hanteras som vi tror eller som avtal säger.
- Risk för många egna anpassningar som utgör risk för informationen som hanteras av tjänsten.
- Risker kopplat till tillgänglighet (och kanske konfidentialitet) eftersom beroende till externa förbindelser (nätleverantörer) finns och blir allt mer centrala för åtkomst till OCI.
- Amerikanskt ägarskap i en alt mer osäker omvärld, risk för informationens konfidentialitet, risk kopplat till tillgänglighet om sanktioner eller tullar innebär för att vi inte får supportpersonal eller andra resurser för att säkra tillgängligheten. Scenario kan vara att amerikanska företag tvingas upphöra i EU.
- Bristande förvaltning och/eller utveckling av befintliga systemstöd innebär ökad risk för informationssäkerheten, exempelvis att systemens tillgänglighet försämras eller att sårbarheter inte åtgärdas i rimlig tid.
- Risk för att Oracle inte fokuserar på följsamhet mot svensk lagstiftning för nya produkter vilket innebär att det tar lång tid att få produkten tillgänglig i Sverige samt mycket egna anpassningar vilket tillsammans utgör risk för informationen som hanteras av tjänsten.
- Osäkerheten i om och när Oracle EHR tillhandahåller det som VGR behöver innebär risk att vi blir kvar med vissa eller stora delar av informationen i IS/IT-tjänster med bristfällig förvaltning och underhåll.
- Migrering i större omfattning innebär risk för informationens riktighet eftersom det krävs mycket tester som kan vara svårt att genomföra i förhållanden som liknar verkligheten.

3. Gör ny upphandling av kärnsystem

(en leverantör av huvuddelen av IT-stödet inom vården)

- Arbetet med Cerner Millennium avbryts och en ny upphandling genomförs
- Målet med denna upphandling är att finna en leverantör av ett kärnsystem inom hälso- och sjukvården (liknande de flesta andra regioner i Sverige)

Risker - alternativ 3

- Många egna anpassningar eftersom det handlar om ett system/monolit som utgör risk för informationen som hanteras av tjänsten.
- Bristande förvaltning och/eller utveckling av befintliga systemstöd innebär ökad risk för informationssäkerheten, exempelvis att systemens tillgänglighet försämras eller att sårbarheter inte åtgärdas i rimlig tid.
- Risk för att leverantören som vinner upphandlingen brister i följsamhet mot svensk lagstiftning vilket tillsammans utgör risk för informationen som hanteras av tjänsten.
- Migrering i större omfattning innebär risk för informationens riktighet eftersom det krävs mycket tester som kan vara svårt att genomföra i förhållanden som liknar verkligheten.
- Om vi hamnar med samma leverantör som stora delar av Sverige ökar risken att sårbarheter utnyttjas. Värdet av sårbarheter ökar för antagonister vilket påverkar informationssäkerheten. Samtidigt finns det större intresse i att aktivt åtgärda sårbarheter i produkten. Samt incitament för samarbete runt att skydda en ”gemensam” miljö ökar
- Risk att VGRs rykte påverkas negativt och leverantörer drar sig från att satsa på utveckling som krävs för att sälja till VGR.
- Stora system har svårt att följa aktuella hot vilket gör att risker inte effektivt kan motverkas eller hanteras av produkten.
- Stora system riskerar att innebära större konsekvenser vid informationssäkerhetsincidenter, svårare att isolera konsekvenser eller drabbad del.

4. Gör nya upphandlingar inom olika områden baserat på openEHR.

- Arbetet med Cerner Millennium avbryts
- Strategiskt väljs openEHR som ramverk för hur vårdinformation ska vara strukturerad
- Upphandlingar av IT-stöd för hälso- och sjukvården genomförs där fokus är på bästa lösningen inom olika behovsområden snarare än ett stort kärnsystem (best-of-breed) med openEHR som gemensam standard. (Likt Region Stockholm)

Risker - alternativ 4

- Bristande förvaltning och/eller utveckling av befintliga systemstöd innebär ökad risk för informationssäkerheten, exempelvis att systemens tillgänglighet försämras eller att sårbarheter inte åtgärdas i rimlig tid.
- Risk att VGRs rykte påverkas negativt och leverantörer drar sig från att satsa på utveckling som krävs för att sälja till VGR.
- Leverantörerna av de olika delarna är troligen känsligare för lågkonjunktur, det kan innebära risk för att systemen inte vidareutvecklas eller underhålls som i sin tur kan påverka informationssäkerheten.
- Risk att VGR inte ges tillräckligt med tid att ställa om
- VGR’s mognadsnivå inom informatik gör att vi inte tillämpar OpenEHR på rätt sätt eller vill göra våld på modellen vilket innebär ökad komplexitet som innebär ökad risk för informationens riktighet och kanske även andra informationssäkerhetsperspektiv.
- Avsaknad av liknande implementationer baserat på OpenEHR i Sverige…

5. Egen utveckling

- Karin Looström Muth bad den regionala arbetsgruppen också ta med alternativet att etablera en förmåga för egen utveckling och på så sätt ta fram den gemensamma vårdinformationsmiljön.
- Detta kom efter det att vi startat vårt arbete, men vi har ändå försökt ta med även detta så bra som möjligt.

Risker - alternativ 5

- Svårt att locka kompetens
- Svårt att behålla kompetens
- Inte mogna för säker utveckling…
- Mycket resurser för att övervaka och säkerställa informationssäkerheten