Granskning av införandet av Min Vård Gävleborg, avseende dataskydd och informationssäkerhet

Region Gävleborg

Mars 2024

Charlotte Arnell, projektledare
Markus Månsson, projektmedarbetare
Sara-Rosa Ageborg, projektmedarbetare
Marie Lindblad, kvalitetssäkrare, certifierad kommunal revisor

pwc

Revisionsrapport

Sammanfattning

Kommuner och regioner har ett av det svenska samhällets mest komplexa uppdrag, detta då en stor del av den samhällsviktiga verksamheten räknas till deras ansvarsområde. En avgörande del av detta uppdrag innebär att hantera information. I många fall är informationen dessutom känslig (både utifrån individen, för organisationen och ibland även utifrån ett risk- och sårbarhetsperspektiv), och i stora volymer.

Revisorerna i Region Gävleborg har identifierat en risk för att införandet av Min Vård Gävleborg och det digitaliseringsarbete som pågår i anslutning till detta, brister avseende efterlevnad av dataskyddsregler och skyddet för personuppgifter. Man har även identifierat en risk för att införandet inte är ändamålsenligt förankrat och riskbedömt.

Sammantaget är vårt intryck att informationssäkerhet och skydd av person-/patientuppgifter är en aktuell och prioriterad fråga inom Region Gävleborg, och som löpande diskuteras. Hälso- och sjukvårdsnämnden har i sin konsekvensbedömning till stor del argumenterat för att plattformens införande är nödvändig och proportionerlig med hänvisning till rättslig reglering, allmännytta och de nyttor som den ökade tillgängligheten och övriga fördelar som en digital hantering innebär. Det framstår även som att diskussionerna i stor utsträckning innefattar balansgången mellan att ta vara på digitaliseringens möjligheter, och skydd för den enskildes integritet. Dock kan vi inte se att diskussionerna är dokumenterad på motsvarande sätt genom utredningar, analyser och beslutshantering.

Vi bedömer att informationsklassningen är genomförd innan driftstart av Min Vård Gävleborg samt att den är ändamålsenlig. Avseende riskanalys och konsekvensbedömning kan det inte verifieras att sådan var genomförd och komplett inför driftstart. Det kan inte heller verifieras att risker analyserats systematiskt under projektet. Det innebär att det finns risk för bristande efterlevnad avseende både interna direktiv och lagstiftning.

Avseende beslutshantering är vår bedömning att det förefaller som att nämnden i relativt liten utsträckning varit involverad i utvecklingen av Min Vård Gävleborg, och inte har kunnat ta ställning till de risker och möjligheter som man utifrån regelverken är ansvarig för. Vi bedömer även att det finns risk för att åtminstone beslut om att godkänna konsekvensbedömning har fattats utan behörighet.

Revisionsfrågor	Bedömning
1. Har införandet av Min Vård Gävleborg hittills varit i linje med gällande lagstiftning och etablerade arbetssätt avseende personuppgiftsbehandling?	Till övervägande del
2. Har införandet av Min Vård Gävleborg hittills genomförts på ett sätt där legala och informationssäkerhetsmässiga risker systematiskt kalibrerats mot de möjligheter och fördelar den nya plattformen kan innebära?	Till övervägande del

Rekommendationer

Mot bakgrund av vad som framkommit i granskningen lämnas följande samlade rekommendationer till hälso- och sjukvårdsnämnden i Region Gävleborg:

- Säkerställa att dokument- och beslutshantering avseende riskanalys och konsekvensbedömning lever upp till kraven avseende ansvarsskyldighet enligt GDPR.
- Säkerställa att beslutshantering inom området följer kommunallagen.
- Säkerställa att identifierade risker omhändertas på ett effektivt sätt.
- Säkerställa att uppföljning/revision av leverantör och uppfyllande av avtalsvillkor sker.

Innehållsförteckning

Förkortningar och begrepp

Asynkront meddelande	Ett asynkront meddelande är en form av kommunikation där sändaren och mottagaren inte behöver vara aktiva samtidigt. I motsats till synkron kommunikation, som exempelvis telefonsamtal eller chatt, kan asynkrona meddelanden skickas och tas emot vid olika tidpunkter. E-post och textmeddelanden är exempel på asynkrona kommunikationsmetoder.
Beaktandesats	EU-lagstiftning inleds normalt med ett antal beaktandesatser. Dessa beskriver skälen till att lagstiftningen tagits fram och används som hjälp för att tolka den efterföljande lagtexten.
Dataskydd	Samlingsbegrepp som både har en formell mening genom dataskyddsförordningen, och för åtgärder som syftar till att skydda personuppgifter.
GDPR	Den allmänna dataskyddsförordningen
HSL	Hälso- och sjukvårdslag
HSN	Hälso- och sjukvårdsnämnden i Region Gävleborg
IMY	Integritetsskyddsmyndigheten
IVO	Inspektionen för vård och omsorg
KL	Kommunallag
LIS	Ledningssystem för informationssäkerhet
MVG	Min Vård Gävleborg
OSL	Offentlighet- och sekretesslag
Personuppgiftsbehandling/ behandling	När personuppgifter hanteras på olika sätt är det formella begreppet för hanteringen ”behandling”. En behandling kan innebära exempelvis insamling, bearbetning, arkivering, spridning eller radering av personuppgifter.
PDL	Patientdatalag
PUB-avtal	Personuppgiftsbiträdesavtal

Inledning

Bakgrund

Kommuner och regioner har ett av det svenska samhällets mest komplexa uppdrag, detta då en stor del av den samhällsviktiga verksamheten räknas till deras ansvarsområde. En avgörande del av detta uppdrag innebär att hantera information. I många fall är informationen dessutom känslig (både utifrån individen, för organisationen och ibland även utifrån ett risk- och sårbarhetsperspektiv), och i stora volymer.

Information, och i synnerhet personuppgifter, inom hälso- och sjukvård är uppgifter som har ett särskilt högt skyddsvärde, både formellt utifrån lagstiftning, och utifrån tradition och kultur. Framför allt beror detta på att informationen många gånger är av en privat natur, och kan dessutom påverka en individ negativt på olika sätt om den blir känd. Det innebär att när hanteringen av sådan information förändras, behöver detta både analyseras och riskbedömas.

Brister i hantering av information och personuppgifter kan leda till ett försämrat förtroende för både den enskilda regionen men även offentlig sektor och välfärdssystemet i allmänhet. Förtroende tar lång tid att bygga upp, men kan snabbt raseras av en enskild incident. Brister kan också leda till skada för organisationen och/eller individerna som drabbas, och i sin tur ge negativa ekonomiska konsekvenser för regionen.

Utifrån digitaliseringen och omvärldsutvecklingen är också informationssäkerhet en avgörande faktor, avseende både säkerhet, förtroende och förmåga till kontinuitet. Det innebär att en region måste försäkra sig om att följa lagar och regler inom området, och arbeta aktivt med utveckling och uppdatering för att hela tiden följa omvärldsutveckling och förändrade förväntningar. Samtidigt innebär digitalisering en mängd möjligheter till både ökad kvalitet och effektivitet. Dessutom är lättillgängliga och smidiga digitala tjänster något som invånarna förväntar sig i allt större utsträckning.

Sammantaget innebär detta att det finns betydande risker både för den försiktiga och konservativa organisationen (exempelvis minskad effektivitet, lägre kvalitet och minskat förtroende från invånare). Men det uppstår också risker för den organisation som digitaliserar och utvecklar nya tjänster och arbetssätt, utan att analysera, riskbedöma, testa och förankra dessa. Detta innebär att det i digitaliseringsarbetet behövs en väl avvägd balans mellan risker och möjligheter. För att nå dit behövs ett systematiskt arbetssätt där både risker och möjligheter kan identifieras och bedömas.

Utifrån ovan resonemang har revisorerna i Region Gävleborg identifierat en risk för att införandet av Min Vård Gävleborg och det digitaliseringsarbete som pågår i anslutning till detta, brister avseende efterlevnad av dataskyddsregler och skyddet för personuppgifter. Man har även identifierat en risk för att införandet inte är ändamålsenligt förankrat och riskbedömt.

Varför är dataskydd och informationssäkerhet viktigt?

Information är i de flesta sammanhang mer eller mindre viktigt, och beroende på sammanhang och omständigheter kan den ha ett mycket högt värde (ofta är värdet högre om den innehåller personuppgifter). Information som delas med obehöriga personer, som ändras av obehöriga eller som inte finns till hands när det behövs kan innebära stora negativa konsekvenser för både en verksamhet och enskilda individer. Bristfällig informationssäkerhet i kritiska verksamhetsfunktioner kan leda till risker för liv och hälsa, för den personliga integriteten och kan även leda till negativ ekonomisk påverkan och förtroendeskada. Informationssäkerhet och dataskydd handlar om att skydda informationen, oavsett var den finns, på ett sätt så att sådana konsekvenser inte uppstår.

Informationssäkerhet kan beskrivas som en uppsättning administrativa och tekniska säkerhetsåtgärder för att bevara informationens konfidentialitet, riktighet och tillgänglighet. Konfidentialitet betyder att informationen är tillgänglig endast för de personer som har behörighet att ta del av den. Riktighet betyder att innehållet i informationen ska vara korrekt och inte kunna förändras av obehöriga. Tillgänglighet betyder att informationen ska vara nåbar när den behövs. Vad som i detta fall konkret utgör behörighet, riktighet och tillgänglighet styrs till största del av lagstiftning, föreskrifter och praxis inom hälso- och sjukvårdsområdet.

Patientuppgifter innehåller ofta både integritetskänslig information och sådana uppgifter som enligt GDPR klassas som känsliga personuppgifter (och därför åtnjuter särskilt lagstadgat skydd). Exempel på integritetskänsliga uppgifter är uppgifter om sociala förhållanden, familjerelationer, uppgifter om barn och vissa ekonomiska uppgifter. Patientuppgifter är generellt också sekretessbelagda enligt OSL, vilket också innebär att de är mer skyddsvärda även utifrån ett dataskyddsrättsligt perspektiv. Exempel på uppgifter som formellt klassas som känsliga är hälsouppgifter, uppgifter om sexualliv och uppgifter om politiska åsikter. Ett bristande dataskydd kan leda till obehörig åtkomst och därmed riskera patientens integritet. Ett robust dataskydd är därför grundläggande för att upprätthålla förtroendet mellan patienter och vårdgivare. Om patienter känner att deras information inte är tillräckligt skyddad, kan det påverka deras vilja att dela viktig information och söka vård, vilket kan i sin tur påverka patientsäkerheten.

Ökad digitalisering innebär en mängd möjligheter, men också att sårbarheter och hot kopplat till dataskydd och informationssäkerhet ökar. Detta medför krav på ökad medvetenhet bland organisationer för att förstå vilken information som är mest kritisk för att bland annat upprätthålla verksamhetsprocesser och säkerställa invånarnas förtroende. Organisationer som hanterar personuppgifter behöver en förmåga att kunna identifiera och skydda dessa, samtidigt som de behöver kunna upptäcka och hantera inträffade incidenter och katastrofer.

Om en organisation väljer att tillgängliggöra information till en extern part, eller möjliggöra användning av till exempel ett IT-system från en tredje part, behöver samma medvetenhet genomsyra leverantörsstyrning och uppföljning. Annars är risken att leverantören blir en sårbarhet för den överlämnande organisationen.

Varför är det viktigt att systematiskt väga risker och möjligheter mot varandra avseende utveckling och personlig integritet?

En systematisk bedömning av risker och möjligheter möjliggör en balans mellan att främja innovation och att skydda personlig integritet. Ett sådant arbetssätt innebär att den ansvariga organisationen över tid kan säkerställa att varken utvecklings- eller integritetsperspektivet väger över och antingen hindrar utveckling till förmån för överdrivet skydd av personlig integritet, eller utsätter organisationen och enskilda för oproportionerliga risker. På så sätt kan både ett balanserat och informerat beslutsfattande ske som gynnar både integritetsskyddet och möjliggör utveckling av arbetssätt och tjänster.

Att enskildas olika rättigheter vägs mot rätten till skydd för sin integritet är också ett arbetssätt som understöds av flera olika regler i GDPR. Exempelvis beskrivs i beaktandesats 4 att ”(...) Rätten till skydd av personuppgifter är inte en absolut rättighet; den måste förstås utifrån sin uppgift i samhället och vägas mot andra grundläggande rättigheter i enlighet med proportionalitetsprincipen.” Vidare beskrivs i artikel 35 p. 7(b) att en konsekvensbedömning ska innehålla ”en bedömning av behovet av och proportionaliteten hos behandlingen i förhållande till syftena.”

Att kunna demonstrera och kommunicera att riskerna kring personlig integritet har vägts mot utvecklingsmöjligheter bidrar generellt också till att skapa förtroende hos både anställda, patienter och anhöriga. Principen om ansvarsskyldighet är också en av de grundläggande principerna i GDPR, och uttrycks enligt följande i artikel 5 p. 2: ”Den personuppgiftsansvarige ska kunna ansvara för och visa att (...) efterlevs”.

Beskrivning av Min Vård Gävleborg

Min Vård Gävleborg är ett kompletterande vårdflöde där bland annat digitala vårdmöten sker. MVG innehåller även tjänster för att underlätta digital kommunikation mellan vård och patient såsom videobesök, asynkrona meddelanden och vårdformulär.

Från patientens perspektiv är MVG en nedladdningsbar app eller hemsida där patienter inom Region Gävleborg kan söka vård oberoende av fysisk lokalisering. När invånare söker vård används ett automatiserat triageringsverktyg. Verktyget kan beskrivas som en digital bedömningstjänst av symtom som ger antingen egenvårdsråd eller rekommendation om att besöka vården. Triageringsverktyget kallas också internt inom Region Gävleborg för triagemotor. Genom att besvara olika frågor inom appen triageras patienten till rätt vårdnivå och typ av vård. Patienten kan hänvisas till akuten, primärvården eller specialistvård och få en rad olika rekommendationer digitalt, vilket möjliggör för ett koncept av tillgänglig och nära vård. Triageringsmodellen är CE-märkt i klass 2A enligt förordning (EU) 2017/745 om medicintekniska produkter.

Rent tekniskt är MVG en plattform, som drivs via en molnlösning. MVG och dess olika funktioner tillhandahålls i nuläget av en och samma leverantör. Triagemotorn har utvecklats i samarbete med Region Gävleborg och fungerar enligt följande:

- Patienten besvarar en rad olika frågor om sitt hälsotillstånd i appen (ett frågeformulär).
- Svaren på frågorna genererar en medicinsk rekommendation. Patienten blir därefter guidad till rätt mottagning eller så får patienten ett egenvårdsråd om besvären bedöms vara så pass milda.
- I vården sorteras ärendet till den mottagning som bedöms bäst kunna hjälpa patienten. Ärendet skickas till vården baserat på:
    - Prioritet;
    - Vårdnivå (primärvård eller specialiserad vård);
    - Besöksform (digitalt eller fysiskt); och
    - Mottagande roll inom vården (yrke, specialitet och spetskompetens).

Syftet är att MVG ska bidra till hälso- och sjukvårdens målsättning om god och jämlik vård. Detta ska ske genom att digital vård ökar tillgängligheten oberoende av plats. Den ökade tillgängligheten ska i sin tur öka jämlikheten mellan patientgrupper och ge bättre förutsättningar att kunna erbjuda anpassad vård utifrån gruppers och individers olika förutsättningar och möjligheter.

Syfte och revisionsfrågor

Granskningen syftar till att bedöma om Region Gävleborg under det hittillsvarande införandet av Min Vård Gävleborg har säkerställt regelefterlevnaden avseende personuppgiftsbehandling samt arbetat på ett ändamålsenligt sätt avseende riskhantering.

Bedömningen görs i huvudsak genom att nedanstående frågeställningar undersöks. Nedan beskrivs även bakgrunden till frågorna och varför de är motiverade att undersöka.

1. Har införandet av Min Vård Gävleborg hittills varit i linje med gällande lagstiftning och etablerade arbetssätt avseende personuppgiftsbehandling?

I huvudsak innebär detta att riskanalyser avseende informationshantering samt konsekvensbedömning enligt GDPR behöver vara genomförda och fastställda innan driftstart. Beroende på leverantörers/personuppgiftsbiträdens tillgång till sekretessbelagda uppgifter behöver även en bedömning göras avseende ett eventuellt röjande av uppgifter gentemot leverantör.

2. Har införandet av Min Vård Gävleborg hittills genomförts på ett sätt där legala och informationssäkerhetsmässiga risker systematiskt kalibrerats mot de möjligheter och fördelar den nya plattformen kan innebära?

Exempel på sådan kalibrering kan vara utredningar där avvägning mellan risker och möjligheter utretts, riskanalyser där det beskrivs hur möjligheter kan väga upp risker eller hur risker kan åtgärdas för att accepteras, eller återkommande analyser och avvägningar så att bedömningarna hela tiden hålls aktuella. Ett annat exempel på ett sådant systematiskt arbetssätt är en beslutsstruktur där avvägningen konsekvent prövas och beslutas om på ett förutsägbart och transparent sätt.

Revisionskriterier

Med revisionskriterier avses de bedömningsgrunder som bildar underlag för analyser och bedömningar i denna granskning.

Kommunallag

I kommunallagen ställs det krav på varje nämnd att inom sitt ansvarsområde se till att verksamheten bedrivs i enlighet med både mål och riktlinjer från fullmäktige och gällande lagstiftning, föreskrifter och liknande. Nämnden måste också ha en tillräckligt god intern kontroll så att den kan säkerställa både följsamhet till mål, interna riktlinjer och lagstiftning, men också att verksamheten även i övrigt bedrivs på ett tillfredsställande sätt.

Den allmänna dataskyddsförordningen (GDPR)

Enligt GDPR måste risk- och konsekvensbedömningar avseende personuppgiftsbehandlingar göras systematiskt. Ett av syftena är att den ansvariga organisationen ska kunna arbeta riskbaserat och anpassa sina åtgärder och skyddsåtgärder utifrån den identifierade risken. Detta innebär att prioritera insatser för att hantera de mest betydande riskerna för fysiska personers integritet och personuppgifternas säkerhet. Den personuppgiftsansvariga organisationen behöver dessutom kunna visa upp dessa analyser och bedömningar för att efterleva lagstiftningen.

Offentlighets- och sekretesslag (OSL)

Den information inom hälso- och sjukvård som rör enskilda patienter är i stor utsträckning sekretesskyddad. Det innebär i sin tur att det också finns särskilda regler för hur informationen behöver hanteras i relation till tekniska hjälpmedel (såsom ett IT-system), leverantörer och liknande. Generellt och något förenklat innebär regelverket, just för hälso- och sjukvård, att alla patientuppgifter ska förutsättas vara sekretessbelagda. Det innebär i sin tur att för att kunna använda sig av en extern part vid hanteringen av de sekretessbelagda uppgifterna, behöver det antingen kunna säkerställas att leverantören inte får tillgång till några sekretessbelagda uppgifter, alternativt att någon av de sekretessbrytande bestämmelserna som finns i OSL är tillämplig.

Lag och förordning om informationssäkerhet för samhällsviktiga och digitala tjänster

Syftet med lagen och tillhörande förordning är att säkerställa en hög gemensam nivå på säkerhet i nätverk och informationssystem, som samhället är beroende av för en trygg och stabil funktionalitet. Alla branscher och sektorer träffas inte av regelverket, men just hälso- och sjukvård är en av de som omfattas, och anledningen är dess viktiga funktion i samhället. Regelverket beskriver bland annat att leverantörer av samhällsviktiga tjänster, som kan vara både från offentlig och privat sektor, ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete, att riskanalyser måste göras och att både organisatoriska och tekniska åtgärder måste vidtas för att

upprätthålla säkerheten. Det ställs även krav på hur incidenter ska hanteras och rapporteras.

Socialstyrelsens föreskrifter och allmänna råd om ledningssystem för systematiskt kvalitetsarbete

Föreskrifterna reglerar hur vårdgivare är skyldiga att systematiskt och fortlöpande arbeta med att utveckla och säkra kvalitet och patientsäkerhet. Bland annat beskrivs hur ledningssystemet behöver vara uppbyggt, vad det systematiska förbättringsarbetet minst måste innehålla (bland annat riskanalyser och kontroll) och hur arbetet ska dokumenteras.

Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården

I föreskrifterna regleras bland annat vad som ska gälla allmänt avseende en vårdgivares informationssäkerhetsarbete (exempelvis ledning av informationssäkerhetsarbete, kontinuitetsarbete och säkerhetskopiering), åtkomst till patientuppgifter, allmänt om hantering av personuppgifter och hur patientjournaler ska struktureras och tas hand om. Reglerna är utformade för att säkerställa patientsäkerhet, integritet och rättssäkerhet.

Avgränsning

Granskningen avgränsas till områdena informationssäkerhet och dataskydd och inriktas på de områden som avser riskhantering och konsekvenshantering. Granskningen är också avgränsad till att omfatta det arbete som gjorts och de åtgärder som vidtagits fram tills dess att MVG togs i skarp användning för vuxna patienter.

Förordningen (EU) 2017/745 om medicintekniska produkter har inte beaktats i denna granskning.

Iakttagelser, bedömningar och rekommendationer baseras endast på den information som tillgängliggjorts under granskningen.

Metod

Granskningen har genomförts genom genomgång av främst relevanta styrande dokument, risk- och sårbarhetsanalyser, informationsklassningar, konsekvensbedömning, samt beslut och beslutsunderlag. Information har inhämtats, genom e-post och vid intervjuer, av följande funktioner;

- Informationssäkerhetschef tillika dataskyddsombud;
- IT-direktör; och
- Projektledare för införandet av Min Vård Gävleborg.

De intervjuade har beretts möjlighet att sakgranska rapporten.

Granskningsresultat

Revisionsfråga 1: Har införandet av Min Vård Gävleborg hittills varit i linje med gällande lagstiftning och etablerade arbetssätt avseende personuppgiftsbehandling?

Iakttagelser

Styrande dokument

I *Direktiv för ansvar och roller* beskrivs hur ansvaret för informationssäkerhetsarbetet ska fördelas och genomföras i organisationen. Det beskrivs att grundprincipen för fördelningen av informationssäkerhetsansvar, följer verksamhetsansvaret. Utöver detta finns även ett informationsägarskap. Detta ägarskap beskrivs vara ett chefsansvar och faller generellt på förvaltningschef, verksamhetschef eller avdelningschef. Avseende projekt beskrivs att projektägare ansvarar för att initial informationsklassning och riskanalys genomförs inför att projekt genomförs. Därefter ansvarar projektledaren för att genomförandet kan ske med tillräcklig säkerhet och att LIS efterlevs.

Direktiv för systematiskt och riskbaserat informationssäkerhetsarbete ger instruktioner för hur regionen ska arbeta med framförallt informationsklassning och riskanalyser gällande informationssäkerhet. I direktivet anges att informationsklassning ska göras inför upphandlingar eller när projekt inleds samt att fördjupad riskanalys även bör göras i samband med detta.

I *Direktiv för informationshantering av extern part* beskrivs förutsättningarna för att regionen ska kunna överlåta information och informationshantering till extern part. Det anges att informationsägaren ansvarar för att direktivet följs. Direktivet anger även att innan en molntjänst används ska informationsklassning och riskanalys ske. Vid behov ska konsekvensbedömning enligt GDPR samt kontinuitetsplanering (i det fall verksamheten förlitar sig på en molntjänst) genomföras.

Direktiv för molntjänster beskriver förutsättningarna för att använda molntjänster i regionens verksamhet samt vilka moment som behöver genomföras innan användning. Av direktivet framgår att chefer och övriga användare av molntjänster ansvarar för att direktivet följs. Det framgår vidare att innan användning av molntjänst påbörjas ska det genomföras klassning av den aktuella informationen samt riskanalys som belyser både risker för verksamheten samt för informationen som behandlas i den aktuella molntjänsten.

I *Inbyggt dataskydd och dataskydd som standard rutin*, anges att den personuppgiftsansvarige måste se till att inbyggt dataskydd och dataskydd som standard tillämpas vid personuppgiftsbehandlingar. Det anges att det är informationsägaren som ansvarar för att rutinen efterlevs. Därefter ges ett antal konkreta exempel på hur inbyggt dataskydd och dataskydd som standard kan implementeras i både arbetssätt och tekniska lösningar, exempelvis minimering av både mängden personuppgifter och lagringstid, begränsad åtkomst till uppgifterna, styrning av användaren i ett system mot ett önskat beteende och möjlighet att inte bli föremål för automatiserat beslutsfattande.

I *Rutin för konsekvensbedömning vid personuppgiftsbehandling* beskrivs syftet med konsekvensbedömningen, att den personuppgiftsansvariga nämnden ansvarar för att rutinen följs samt att konsekvensbedömningen ska genomföras före en personuppgiftsbehandling sker, och därefter en gång per år. Därefter beskrivs i vilka situationer som en konsekvensbedömning behöver göras, samt biläggs en mall för själva bedömningen.

I hälso- och sjukvårdsnämndens eller regionstyrelsens respektive *delegationsordningar* framgår inte att delegation ges avseende riskanalyser, konsekvensbedömningar eller liknande.

De ovan redovisade styrande dokumenten är inte konsekvent eller fullständigt daterade varför det i vissa fall är något oklart när de började gälla eller om de fortfarande gäller.

Informationsklassning och riskanalys

Enligt intervjuer har en informationskartläggning med tillhörande klassning av informationen genomförts inför driftstart av MVG. Vi har fått ta del av ett dokument som innehåller kartläggning och klassning avseende information inom ramen för den digitala vårdkedjan. Dokumentet är inte daterat men är utskrivet den 16 maj 2019 och får därmed antas vara framtaget i projektets initiala skede.

Avseende riskanalyser gör vi följande iakttagelser;

- Under intervjuer beskrivs att riskanalyser avseende personuppgiftsbehandling och konsekvensbedömning enligt GDPR har genomförts inför driftstart av MVG. Vi har också fått ta del av dessa dokument. Riskanalysen är integrerad med konsekvensbedömningen i ett dokument. Vi kan dock inte verifiera att riskanalys och konsekvensbedömning är fastställd och genomförd innan driftstart eftersom dokumentet inte är daterat. Det enda datumet som förekommer i dokumentet är datum för hälso- och sjukvårdsdirektörens beslut att fastställa och godkänna konsekvensbedömningen, vilket är den 26 juni 2023.
- Riskanalysen vi tagit del av inkluderar identifierade risker, beskrivning av konsekvenser, allvarlighetsgrad, sannolikhet samt handlingsplan för att hantera riskerna. I några enstaka fall framgår att risken är åtgärdad men i de flesta fall är ett datum noterat för när risken ska vara åtgärdad, alternativt att det anges att den ska åtgärdas kontinuerligt eller så är fältet blankt.
- Utöver den riskanalys som gjorts avseende personuppgiftsbehandling så har projektrelaterade risker analyserats inom hälso- och sjukvårdens olika verksamhetsområden under projektet. I dessa riskanalyser har dock risker relaterat till informationssäkerhet och dataskydd inte inkluderats i någon större utsträckning.
- Under intervjuerna framkommer att risker relaterat till informationssäkerheten för MVG har beaktats och hanterats kontinuerligt under projektets gång samt att relevanta roller (såsom informationssäkerhetschef) varit involverade under projektet.
- Utifrån de underlag som tillhandahållits i granskningen så kan vi inte verifiera att riskhantering avseende informationssäkerhet har genomförts systematiskt och regelbundet under projektet. En sådan systematisk riskhantering hade exempelvis

kunnat vara dokumenterade uppföljningar av de identifierade riskerna, förnyade konsekvensbedömningar eller liknande.

- I samband med denna granskning har vi mottagit en redogörelse för hur de identifierade riskerna har omhändertagits. Det beskrivs att de allra flesta riskerna är hanterade. Dock kan vi i vissa fall fortfarande inte verifiera att så är fallet genom exempelvis dokumentation.

- Flera av riskerna är hänförliga till leverantören av plattformen, Doktor 24 Healthcare AB. Exempel på sådana risker är att leverantören använder personuppgifter för egna ändamål och att hårdvara används på felaktigt sätt. I redogörelsen för hur dessa risker har åtgärdats hänvisas till PUB-avtalet mellan leverantören och regionen. Vi har tagit del av PUB-avtalet och kan därigenom verifiera att riskerna är omhändertagna genom avtalet. Däremot har vi inte kunnat få tydligt svar på om regionen har följt upp hur leverantören efterlever avtalet, eller om en revision hos leverantören har genomförts.

Konsekvensbedömning enligt GDPR

Avseende konsekvensbedömningen gör vi följande iakttagelser;

- I konsekvensbedömningen anges HSN som personuppgiftsansvarig.

- MVG innehåller en teknisk utveckling, framförallt den digitala triageringen. I konsekvensbedömningen beskrivs den som en “automatisk process för att triagera patienter inför kontakt med vårdgivaren”. Det uppges också i konsekvensbedömningen att MVG innebär användning av ny teknik. Dock kan vi inte se att den automatiska triageringen, och den personuppgiftsbehandling som den innebär, analyseras avseende proportionalitet och skälighet.

- Av konsekvensbedömningen framgår att det inte finns någon framtagen metod för radering och/eller gallring av personuppgifter i plattformen. Det anges att detta ska tas fram i samråd med regionarkivet. Vid intervjuerna framkommer att detta inte är åtgärdat vilket innebär att personuppgifter och andra uppgifter finns kvar i plattformen. Det anges också i konsekvensbedömningen att uppgifter som utgör vårdinformation manuellt ska kopieras från plattformen till journalsystemet. Dock framgår inte om och i så fall hur uppgifter raderas från plattformen.

- Enligt konsekvensbedömningen saknas rutiner för att sektionera behörighetsnivåer i MVG. Den beskrivna handlingsplanen anger att detta ska åtgärdas och eventuellt ska det kravställas på leverantören att ta fram teknisk möjlighet för detta. Vi har tagit del av dokumentet *Rätt att ta del av patientuppgifter - Rutin, Hälso och sjukvård, Region Gävleborg* som beskriver behörighetshanteringen generellt avseende hälso- och sjukvårdsverksamheten. Däremot har vi inte kunnat verifiera hur de olika behörighetsnivåerna hanteras i MVG eller om förändring av tekniska möjligheter har skett.

- Dataskyddsombudet har getts möjlighet att yttra sig om konsekvensbedömningen inklusive riskanalysen. Dataskyddsombudets bedömning är att de registrerade kan tillgodogöra sig sina rättigheter och att personuppgiftsansvarig uppfyller sina skyldigheter, men att en del risker kvarstår att hanteras. Riskerna som nämns avser

teknisk behörighetsstyrning, svårigheter för medarbetare att hantera plattformen på ett korrekt sätt samt säkerheten för patientuppgifter. Det framgår inte av konsekvensbedömningen, och vi har inte kunnat verifiera det på annat sätt, hur dessa påpekanden från dataskyddsombudet har omhändertagits.

- Konsekvensbedömningen är fastställd av hälso- och sjukvårdsdirektören. Vi har inte kunnat verifiera att beslut om att fastställa konsekvensbedömning finns varken i delegationsordning eller i särskilt beslut om delegation. Av *Rutin för konsekvensbedömning vid personuppgiftsbehandling* framgår inte vem som ska fastställa konsekvensbedömningen, endast att den personuppgiftsansvariga (HSN i detta fall) ansvarar för att den blir genomförd.

Personuppgiftsbiträdesavtal

Regionen har tecknat PUB-avtal med leverantören av plattformen och appen som ska möjliggöra den digitala vårdkedjan, Doktor 24 Healthcare AB. Avtalet är undertecknat i mars 2020 och har således kommit på plats innan MVG börjat användas i skarpt läge (vilket är obligatoriskt enligt GDPR).

Bedömning

Har införandet av Min Vård Gävleborg hittills varit i linje med gällande lagstiftning och etablerade arbetssätt avseende personuppgiftsbehandling?

Svar: Till övervägande del

Informationsklassning och riskanalys

Vi bedömer att informationsklassningen är genomförd både innan driftstart av MVG samt att den är ändamålsenlig. Till övervägande del bedömer vi att innehållet i riskanalysen är fullständigt och ändamålsenligt. Det kan dock inte verifieras att den är fastställd innan driftstart eftersom den är godkänd i juni 2023. Det kan inte heller verifieras att risker analyserats systematiskt under projektet. Det innebär att det finns risk för bristande efterlevnad avseende både interna direktiv och lagstiftning.

Avseende riskanalyserna gör vi även följande bedömning;

- Vi bedömer det finns ett antal handlingsplaner som inte är helt ändamålsenliga och effektiva. Exempel på sådan handlingsplan är att “Leverantören ska etablera och upprätthålla en informationssäkerhet som skyddar mot intrång” för att hantera risken att obehöriga får tillgång till personuppgifterna i plattformen. Handlingsplanen beskriver därmed snarare en målsättning, men bör vara mer konkret för att på ett ändamålsenligt sätt hantera risken.

- Det samlade intrycket är att riskanalysen inte är helt färdigställd. Anledningen är att det inte framgår av riskanalysen, eller av annat dokument vi fått tillgång till, om de identifierade riskerna är åtgärdade i enlighet med handlings- och tidsplan. Under intervjuerna har vi inte kunnat få svar på hur riskerna har omhändertagits. Efter intervjuerna har vi fått en skriftlig redogörelse för hur verksamheten anser sig ha

omhändertagit och åtgärdat riskerna. Det är positivt, men innebär inte att det går att styrka att ett systematiskt och dokumenterat riskarbete har bedrivits.

- Sammantaget bedömer vi att det finns risk för att regionen inte har full kontroll på de identifierade riskerna, vilket i sin tur innebär risk för att interna direktiv och lagstiftning inte efterlevs.

Konsekvensbedömning enligt GDPR

Till övervägande del bedömer vi att konsekvensbedömningen uppfyller kraven i GDPR. Det samlade intrycket är att bedömningen är relativt fullständig och ändamålsenlig. Vi noterar dock några brister och oklarheter;

- Vi kan inte verifiera att riskanalys och konsekvensbedömning är fastställd och genomförd innan driftstart eftersom dokumentet är fastställt och godkänt i juni 2023. Detta bedöms som en brist eftersom både regionens interna direktiv och lagstiftning ställer krav på att dessa genomförs innan den aktuella personuppgiftsbehandlingen påbörjas.

- MVG innehåller en betydande teknisk utveckling, framför allt den digitala triageringen. Den digitala triageringen innebär sannolikt inte att fler, eller annorlunda, typer av personuppgifter behandlas. Däremot behandlas de på ett nytt sätt. I konsekvensbedömningen beskrivs också att ny teknik används och att det är fråga om automatiskt beslutsfattande. För att konsekvensbedömningen skulle ha bedömts som helt ändamålsenlig bedömer vi att dessa aspekter hade behövt belysas och analyseras i större utsträckning.

- Vi bedömer att det finns en risk för att patientinformation (som både utgör känsliga personuppgifter och sekretessbelagd information) lagras längre än nödvändigt i MVG. Anledningen är att vi inom ramen för granskningen inte kunnat verifiera att patientuppgifter raderas från plattformen efter att de överförts till journalsystemet.

- Utifrån att det i övrigt framstår som relativt oklart hur identifierade risker har omhändertagits hade det varit önskvärt med en större tydlighet kring hur dataskyddsombudets yttrande har omhändertagits. Det hade också varit önskvärt med ett resonemang kring varför hälso- och sjukvårdsdirektören fattat beslut om att gå vidare med införandet av plattformen, trots de risker som dataskyddsombudet framför. Bristen på dokumenterad argumentation och på dokumentation avseende hur risker har omhändertagits innebär en risk för att konsekvensbedömningen inte skulle anses som tillräcklig.

- Mot bakgrund av att vi inte kunnat verifiera att delegation finns för beslutet att fastställa konsekvensbedömningen, eller att det i annat styrande dokument framgår att det är hälso- och sjukvårdsdirektören som ska fatta beslutet, är vår bedömning att det finns risk för att hälso- och sjukvårdsdirektörens beslut är fattat utan behörighet. Det innebär också att det finns risk att det tagits ett beslut på ett sätt som omöjliggör överklagande, i ett fall där en sådan möjlighet borde ha funnits (se vidare resonemang i denna fråga under bedömning avseende revisionsfråga 2).

Personuppgiftsbiträdesavtal

Bedömningen är att PUB-avtalet innehåller de obligatoriska delar som ett sådant avtal måste innehålla enligt GDPR art. 28. Bedömningen är också att de instruktioner som ges till personuppgiftsbiträdet, och som denne är bunden att följa, i allt väsentligt är ändamålsenliga för att de krav som ställs i GDPR ska uppfyllas.

Revisionsfråga 2: Har införandet av Min Vård Gävleborg hittills genomförts på ett sätt där legala och informationssäkerhetsmässiga risker systematiskt kalibrerats mot de möjligheter och fördelar den nya plattformen kan innebära?

Iakttagelser

Styrande dokument

I *Programdirektiv PO 1 Digitala vårdmöten* anges att det ska göras en SWOT-analys av införandet av digitala vårdmöten. Analysen ska göras i styrgruppen för programområdet. Det anges vidare att riskanalyser ska göras inom ramen för de olika projekten. I övrigt se iakttagelser under revisionsfråga 1.

De styrdokument vi har tagit del av styr generellt mot en hantering av risker. Vi har inte tagit del av styrande dokument som ger direktiv eller vägledning kring hur både möjligheter och risker ska hanteras i relation till varandra.

I hälso- och sjukvårdsnämndens och regionstyrelsens respektive *delegationsordningar* framgår inte att delegation ges avseende riskanalyser eller liknande.

Riskanalys och konsekvensbedömning enligt GDPR

En konsekvensbedömning enligt GDPR ska innehålla en redogörelse och bedömning av huruvida de planerade personuppgiftsbehandlingarna är proportionerliga i relation till det syfte som avses att uppnås med behandlingen (det vill säga möjligheten). Den aktuella konsekvensbedömningen innehåller en sådan redogörelse och analys.

I konsekvensbedömningen beskrivs att ett av ändamålen med MVG är att regionen i större utsträckning ska uppfylla hälso- och sjukvårdslagens och patientlagens krav om att vården ska främja goda kontakter mellan patient och hälso- och sjukvårdspersonal, vara lättillgänglig samt att patienter snarast ska få medicinska bedömningar av sina hälsotillstånd. Det beskrivs också att digitala vårdbesök kan ge större kostnadseffektivitet eftersom vårdgivaren kan använda lokaler på ett mer effektivt sätt.

I viss utsträckning innehåller även riskanalysen en dokumenterad avvägning mellan möjlighet och risk. Ett sådant exempel är bedömningen avseende sektionering av behörighetsnivåer. Där lyfts fram både risken att en medarbetare får tillgång till för mycket personuppgifter, och risken som uppstår om tillgången begränsas (nämligen att medarbetaren saknar tillgång till nödvändiga uppgifter).

Förankring och beslutshantering

MVG är en del i arbetet med utvecklingen av god och nära vård, och enligt uppgift från regionen fattades det första beslutet i HSN avseende god och nära vård

under 2018. Den 5 april 2018 gavs i uppdrag till hälso- och sjukvårdsdirektören att genomföra en fördjupad analys avseende åtgärder som stöder utvecklingen av en modern, jämlik, tillgänglig och effektiv hälso- och sjukvård med fokus på den nära vården. Den 12 december 2018 informerades nämnden bland annat om att en så kallad digital vårdkedja planerades bli en del av utvecklingen av god och nära vård. Den 16 januari 2019 beslutade HSN att arbetet med god och nära vård skulle fortsätta i enlighet med den tidigare beslutade och föreslagna inriktningen.

Den 21 september 2020 informerades HSN om att ett system för digitala vårdmöten är upphandlat. Den 11 november 2020 informerades HSN om att vårdtjänster kommer att införas via en digital plattform.

I övrigt har vi inte kunnat verifiera att något ärende om MVG har beslutats om i HSN, såsom ett godkännande att gå vidare i projektet utifrån en fastslagen riskanalys, godkännande av konsekvensbedömning eller liknande.

Vi har inte fått del av beslutslogg, protokoll eller motsvarande från projektets styrgrupp eller liknande, där avvägning mellan risker och möjligheter har beslutats eller diskuterats. Vi har inte heller kunnat verifiera om det har funnits en bestämd ordning inom ramen för projektet hur den typen av frågor ska hanteras. Det innebär att vi inte kunnat granska hur frågor om avvägning mellan risker och möjligheter avseende informationssäkerhet och dataskydd skett.

Intervjuer

Vid intervjuerna beskrivs att arbetet med MVG har varit riskbaserat och att bedömningar avseende risk kontra möjligheter gjorts kontinuerligt. Det framhålls även att det är en mogen organisation i dessa frågor och att det pågår kontinuerliga diskussioner avseende MVG och informationssäkerhet och dataskydd. Det beskrivs även att arbetet med MVG har präglats av noggrannhet och ett högt säkerhetsmedvetande.

Bedömning

Revisionsfråga 2: Har införandet av Min Vård Gävleborg hittills genomförts på ett sätt där legala och informationssäkerhetsmässiga risker systematiskt kalibrerats mot de möjligheter och fördelar den nya plattformen kan innebära?

Svar: Till övervägande del

HSN har i konsekvensbedömningen till stor del argumenterat för att plattformens införande är nödvändig och proportionerlig med hänvisning till rättslig reglering, allmännytta och de nyttor som den ökade tillgängligheten och övriga fördelar som en digital hantering innebär. Sammantaget innehåller konsekvensbedömningen i allt väsentligt en gedigen redogörelse kring nyttan av digitalisering och olika typer av personuppgiftsbehandlingar inom hälso- och sjukvård.

Analysen tenderar dock att vara en avvägning mellan den enskildes integritet och personuppgiftsbehandling inom hälso- och sjukvård överlag. Exempelvis lyfts lagkrav

om att hälso- och sjukvård måste administreras på ett sätt som säkerställer god kvalitet och att man har en skyldighet att erbjuda vård utifrån patientens förutsättningar. Det saknas dock i stor utsträckning resonemang och analys kring hur de specifika fördelarna och möjligheterna med MVG överväger de integritetsrisker som uppstår med den typen av personuppgiftsbehandlingar som införs, utökas och förändras i och med införandet av MVG.

Av intervjuerna framgår att frågan om informationssäkerhet och skydd av person-/patientuppgifter är levande inom Region Gävleborg. Det framstår även som att dessa diskussioner i stor utsträckning innefattar balansgången mellan att ta vara på digitaliseringens möjligheter, och skydd för den enskildes integritet. Dock kan vi inte se att denna diskussion är dokumenterad på samma sätt genom utredningar, analyser och beslutshantering. Det innebär sammantaget att det finns en risk för att utvecklingsarbetet inte sker på ett tillräckligt transparent sätt, vilket på lång sikt kan påverka utvecklingsarbetet negativt. Det innebär också en risk för formella sanktioner, främst kopplat till efterlevnaden av GDPR. Anledningen är att ett grundläggande krav i lagstiftningen är att den personuppgiftsansvariga organisationen i alla lägen ska kunna visa att och hur man efterlever lagkraven. En del i den demonstrationen avser att kunna visa hur risker och möjligheter balanseras mot varandra.

De interna styrdokumenten anvisar ansvar för olika uppgifter och moment till både “personuppgiftsansvarig”, det vill säga ansvarig nämnd, och till tjänstepersoner. Det yttersta ansvaret för personuppgiftsbehandling faller dock alltid på den personuppgiftsansvarige, vilket är HSN i detta fall. HSN har även verksamhetsansvaret och ansvar enligt kommunallagen att säkerställa att verksamheten bedrivs i enlighet med relevant lagstiftning. Detta innebär att det är HSN som både “äger” risker, möjligheter och ansvaret för dessa. Utifrån det material vi fått tillgång till under granskningen gör vi bedömningen att det finns risk för att nämnden inte har kunnat utöva det ägandeskapet. Anledningen är att det förefaller som att nämnden i relativt liten utsträckning varit involverad i utvecklingen av MVG, och inte har kunnat ta ställning till de risker och möjligheter som man utifrån regelverken är ansvarig för.

Avsaknaden av beslut i nämnden, samt avsaknad av delegerade beslut, innebär att de flesta av besluten kopplat till införandet av MVG till synes har fattats av tjänstepersoner genom så kallade verkställighetsbeslut. Verkställighetsbeslut kännetecknas bland annat av att det inte får finnas utrymme för självständiga bedömningar och besluten grundas på arbetsfördelning i verksamheten. Om beslutet innebär en bedömning, vägval eller avvägning mellan olika alternativ och intressen innebär det generellt att beslutet är ett så kallat ”beslut i kommunallagens mening”. Då måste beslutet tas av nämnd eller på delegation, och det är också möjligt att överklaga beslutet genom laglighetsprövning. Vissa beslut får heller inte delegeras enligt kommunallagen, exempelvis beslut om verksamhetens mål, inriktning eller kvalitet. Av förarbetena till kommunallagen sägs, vilket är den uppfattning som också stöds i praxis, att rent förberedande åtgärder eller rent verkställande åtgärder där det saknas utrymme för självständiga bedömningar inte är beslut i kommunallagens mening. Beslut där det föreligger alternativa lösningar och beslutsfattaren själv måste göra vissa överväganden eller bedömningar anses däremot utgöra beslut i kommunallagen mening.

Beslutet i detta fall innebär att de bedömningar och risknivåer som beskrivs i konsekvensbedömningen accepteras, och att det bedöms att de registrerade kan tillgodogöra sig sina rättigheter och att personuppgiftsansvarig uppfyller sina skyldigheter. Det är ett komplext beslut, särskilt då både stora volymer av känsliga personuppgifter behandlas och ny teknik används. Därför bedömer vi inte att det handlar om verkställighet, utan om ett beslut i kommunallagens mening. Det innebär att beslutet måste fattas av nämnden eller på delegation av densamma.

Ett av syftena med det regelverk som gäller för beslutsfattande i regioner är också att möjliggöra insyn i och kring beslut, samt att de ska vara möjliga att överklaga för regionmedlemmar. Om beslut fattas på tjänstemannanivå, där de riskerar att inte bli kända för regionmedlemmarna och inte vara möjliga att överklaga, i allt för stor omfattning, riskerar regionen att tappa förtroendet från sina invånare. I just frågor kopplat till integritet och digitalisering brukar användarnas förtroende lyftas som en av de viktigaste framgångsfaktorerna. Även regionen själv lyfter fram användarnas förtroende, och förlorande av det, som en risk i konsekvensbedömningen. I ljuset av detta framstår det som angeläget att transparens och tydligt beslutsfattande prioriteras i den här typen av utvecklingsprocesser.

Samlad bedömning

Vi bedömer att informationsklassningen är genomförd innan driftstart av MVG samt att den är ändamålsenlig. Avseende riskanalys och konsekvensbedömning kan det inte verifieras att sådan är genomförd och komplett inför driftstart av MVG. Det kan inte heller verifieras att risker analyserats systematiskt under projektet. Det innebär att det finns risk för bristande efterlevnad avseende både interna direktiv och lagstiftning.

Till övervägande del bedömer vi att konsekvensbedömningen uppfyller kraven i GDPR. Det samlade intrycket är att riskanalys och konsekvensbedömning till övervägande del är fullständig och ändamålsenlig. Bedömningen är att PUB-avtalet innehåller de obligatoriska delar som ett sådant avtal måste innehålla enligt GDPR.

Sammantaget är vårt intryck att informationssäkerhet och skydd av person-/patientuppgifter är en aktuell och prioriterad fråga inom Region Gävleborg. HSN har i konsekvensbedömningen till stor del argumenterat för att plattformens införande är nödvändig och proportionerlig med hänvisning till rättslig reglering, allmännytta och de nyttor som den ökade tillgängligheten och övriga fördelar som en digital hantering innebär. Det framstår även som att dessa diskussioner i stor utsträckning innefattar balansgången mellan att ta vara på digitaliseringens möjligheter, och skydd för den enskildes integritet. Dock kan vi inte se att dessa diskussioner är dokumenterade på samma sätt genom utredningar, analyser och beslutshantering.

Avseende beslutshantering är vår bedömning att det förefaller som att nämnden i relativt liten utsträckning varit involverad i utvecklingen av Min Vård Gävleborg, och inte har kunnat ta ställning till de risker och möjligheter som man utifrån regelverken är ansvarig för. Vi bedömer även att det finns risk för att åtminstone beslut om att godkänna konsekvensbedömning har fattats utan behörighet.

Revisionsfrågor	Bedömning
1. Har införandet av Min Vård Gävleborg hittills varit i linje med gällande lagstiftning och etablerade arbetssätt avseende personuppgiftsbehandling?	Till övervägande del
2. Har införandet av Min Vård Gävleborg hittills genomförts på ett sätt där legala och informationssäkerhetsmässiga risker systematiskt kalibrerats mot de möjligheter och fördelar den nya plattformen kan innebära?	Till övervägande del

12 mars 2024

Karin Magnusson
Uppdragsledare

Charlotte Arnell
Projektledare
