BÄSTA LIVSPLATSEN
Region Halland

Regionens revisorer 2025-04-10

Till Regionstyrelsen

Regionfullmäktiges presidium för kännedom

Revisionsrapport Granskning av hantering av personuppgifter och sekretess vid digitala vårdmöten

Regionens revisorer har vid sitt sammanträde 2025-04-10 behandlat och godkänt bifogad revisionsrapport Granskning av hantering av personuppgifter och sekretess vid digitala vårdmöten.

Granskningens syfte är att bedöma om regionstyrelsen har säkerställt att digitala vårdmöten sker på ett ändamålsenligt och lagenligt sätt. Vi har i vår granskning biträtts av sakkunniga från PwC.

Utifrån genomförd granskning är vår samlade bedömning att regionstyrelsen inte helt har säkerställt att digitala vårdmöten sker på ett ändamålsenligt och lagenligt sätt.

Utifrån granskningen iakttagelser lämnas följande rekommendationer till regionstyrelsen:

- Säkerställa att riskanalyser, konsekvensbedömningar enligt GDPR och lämplighetsbedömningar enligt OSL snarast genomförs,
- Säkerställa att lämplighetsbedömningar dokumenteras på ett sätt som innebär att det är tydligt att bedömningar har skett innan utlämning (det vill säga innan en tjänst tagits i bruk), och att OSL därmed efterlevs,
- Säkerställa att de brister och oklarheter avseende främst tjänsteavtal och dess koppling till PUB-avtal åtgärdas vid liknande anskaffningar framgent,
- Säkerställa att uppföljning av leverantörer och avtal initieras snarast, samt att ett systematiskt arbetssätt avseende uppföljning inom området etableras,
- Säkerställa att ett systematiskt arbetssätt etableras (kan med fördel göras genom användning av utvecklad teknik), som innebär att registerförteckningarna regelbundet uppdateras och kvalitetssäkras,
- Säkerställa att ändamålsenliga rutiner finns även på systemspecifik nivå,
- Säkerställa att väl anpassad information om personuppgiftsbehandling sker på ett lättillgängligt sätt vid digitala vårdmöten.

Yttrande samt redogörelse om vilka åtgärder regionstyrelsen avser att vidta med anledning av resultatet i granskningen önskas senast 2025-08-10.

För regionens revisorer

Lillemor Landén Vepsä
Ordförande

Bilaga: Revisionsrapport Granskning av hantering av personuppgifter och sekretess vid digitala vårdmöten.

Svar sänds till: regionen@regionhalland.se

Granskning av hantering av personuppgifter och sekretess vid digitala vårdmöten

Region Halland

April 2025

Charlotte Arnell, projektledare

Agnes Westerlund, projektmedarbetare

Marie Lindblad, kvalitetssäkrare

pwc

Revisionsrapport

Sammanfattning

PwC har på uppdrag av de förtroendevalda revisorerna i Region Halland genomfört en granskning av hanteringen av personuppgifter och sekretess vid digitala vårdmöten. Granskningens syfte är att bedöma om regionstyrelsen har säkerställt att digitala vårdmöten sker på ett ändamålsenligt och lagenligt sätt.

Utifrån genomförd granskning är vår samlade bedömning att regionstyrelsen **inte helt** har säkerställt att digitala vårdmöten sker på ett ändamålsenligt och lagenligt sätt.

Granskningen visar att regionen inte har genomfört och dokumenterat varken riskanalys, konsekvensbedömning eller lämplighetsbedömning, på ett fullständigt sätt för någon av de tjänster som är godkända att använda för digitala vårdmöten. Detta skapar en betydande risk både för informationssäkerheten och för att regionen inte uppfyller GDPR och OSL. Däremot är det positivt att analyser och bedömningar åtminstone påbörjats för Visiba Care, där förnyad användning och avtal aktualiserats under 2025. Granskningen visar också att medvetenhet om vikten av att hantera personuppgifter och sekretessbelagd information finns, vilket är positivt.

Det är också positivt att både tjänste- och PUB-avtal finns för alla tjänster. De är i stora delar ändamålsenliga men innehåller till viss del brister i form av ofullständiga instruktioner samt oklarheter avseende olika avtalsparter. Avtalen med leverantörer tillhandahåller villkor för uppföljning, men regionen saknar ett systematiskt arbetssätt för att kontrollera leverantörernas avtalsefterlevnad. Detta försvårar leverantörskontrollen, vilket innebär en ökad risk för säkerhetsbrister.

Registerförteckningen av personuppgiftsbehandlingar uppfyller kraven i GDPR på en övergripande nivå men det är otydligt hur pass uppdaterat registret är. När det gäller rutiner och annan vägledning för hur patientuppgifter och annan sekretessbelagd information får hanteras inom regionen vid digitala vårdmöten, bedömer vi att dessa till viss del är ändamålsenliga. Dock saknas i vissa fall specifika rutiner och i vissa fall saknas instruktioner helt. Vi bedömer att den informationen som ges avseende personuppgiftsbehandling på generell nivå inom regionen är väl anpassad, men däremot är det svårt för patienter och anhöriga att på ett lättillgängligt sätt få fullständig information om hanteringen av deras personuppgifter vid specifikt digitala vårdmöten.

Nedan ses bedömning för varje revisionsfråga. För fullständiga bedömningar, se respektive revisionsfråga i rapporten.

Revisionsfrågor	Bedömning	
Har ändamålsenlig riskanalys, konsekvensbedömning och lämplighetsbedömning genomförts innan implementering?	Nej	
Finns ändamålsenligt tjänste- och personuppgiftsbiträdesavtal med leverantören av tjänsten?	Delvis	
Är de personuppgiftsbehandlingar som digitala vårdmöten innebär, korrekt införda i regionstyrelsens registerförteckning över personuppgiftsbehandlingar?	Delvis	
Har tjänsten följts upp på ett ändamålsenligt sätt, avseende skydd av sekretessbelagda uppgifter och personuppgifter?	Delvis	
Finns interna regler, rutiner och vägledning som reglerar och stödjer användningen av digitala vårdmöten?	Delvis	
Ges patienter och anhöriga information om behandlingen av deras personuppgifter vid de digitala vårdmötena i enlighet med gällande lagstiftning?	Delvis	

Rekommendationer

Regionstyrelsen rekommenderas att:

- Säkerställa att riskanalyser, konsekvensbedömningar enligt GDPR och lämplighetsbedömningar enligt OSL snarast genomförs,
- Säkerställa att lämplighetsbedömningar dokumenteras på ett sätt som innebär att det är tydligt att bedömningar har skett innan utlämning (det vill säga innan en tjänst tagits i bruk), och att OSL därmed efterlevs,
- Säkerställa att de brister och oklarheter avseende främst tjänsteavtal och dess koppling till PUB-avtal åtgärdas vid liknande anskaffningar framgent,
- Säkerställa att uppföljning av leverantörer och avtal initieras snarast, samt att ett systematiskt arbetssätt avseende uppföljning inom området etableras,
- Säkerställa att ett systematiskt arbetssätt etableras (kan med fördel göras genom användning av utvecklad teknik), som innebär att registerförteckningarna regelbundet uppdateras och kvalitetssäkras,
- Säkerställa att ändamålsenliga rutiner finns även på systemspecifik nivå,
- Säkerställa att väl anpassad information om personuppgiftsbehandling sker på ett lättillgängligt sätt vid digitala vårdmöten.

Innehållsförteckning

Förkortningar och begrepp

Digitalt vårdmöte	Möte med patient via video. I Region Halland används begreppet videobesök eller besök via video.
GDPR	Den allmänna dataskyddsförordningen EU (2016/679)
HSLF-FS 2016:40	Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården
Informations-säkerhet	Det finns ingen legal eller formellt fastslagen definition av informations-säkerhet. En vedertagen beskrivning däremot är att informationssäkerhet utgörs av en uppsättning administrativa och tekniska åtgärder för att bevara informationens konfidentialitet, riktighet och tillgänglighet. Konfidentialitet innebär att informationen endast är tillgänglig för behöriga personer. Riktighet innebär att informationens innehåll är korrekt och inte kan ändras av obehöriga. Tillgänglighet innebär att informationen är tillgänglig när den behövs.
IMY	Integritetsskyddsmyndigheten
IT-säkerhet	Det finns ingen legal eller formellt fastslagen definition av IT-säkerhet. En vanlig beskrivning är att IT-säkerhet avser de tekniska delarna av informationssäkerhet, både avseende IT och fysisk säkerhet. IT-säkerhet handlar om allt från vpn-förbindelser och antivirus till intrångsdetektering och säkerhetskopiering.
Molntjänst	En molntjänst är en IT-tjänst som levereras över internet, vilket möjliggör lagring, delning och åtkomst av data utan att behöva lagra den lokalt på en enhet.
MSBFS 2018:8	Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster.
OSL	Offentlighets- och sekretesslag (2009:400)
Personuppgifts-behandling/ behandling	Med behandling av personuppgifter menas i princip allting som går att göra med personuppgifterna. Det kan till exempel vara att samla in, registrera eller lagra uppgifterna.
PUA	Personuppgiftsansvarig är den organisation som bestämmer för vilka ändamål personuppgifter ska behandlas och hur behandlingen ska gå till. Inom Region Halland är varje nämnd och styrelse personuppgiftsansvarig för de personuppgiftsbehandlingar som sker inom respektive verksamhet.
PUB	Personuppgiftsbiträde är den som behandlar personuppgifter för den personuppgiftsansvariges räkning, exempelvis leverantörer som behandlar personuppgifter på regionens uppdrag och instruktioner.
PUB-avtal	Personuppgiftsbiträdesavtal. Avtalet är obligatoriskt enligt GDPR och reglerar hur biträdets behandling av personuppgifter ska gå till.
Underbiträde	Underbiträde är den som behandlar personuppgifter för personuppgifts-biträdets räkning. När ett personuppgiftsbiträde anlitar ett underbiträde måste de teckna avtal som gör att biträdet omfattas av samma skyldigheter som personuppgiftsbiträdet har gentemot den personuppgiftsansvariga.
SKR	Sveriges Kommuner och Regioner

Inledning

Bakgrund

Regionerna 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 personuppgifter av olika slag. I många fall kan uppgifterna vara både sekretessbelagda och känsliga, och i stora volymer.

Digitala vårdmöten erbjuder många fördelar, men det finns också potentiella risker som måste hanteras för att säkerställa patienternas säkerhet och integritet. Sådana risker kan exempelvis vara relaterade till säkerhet, integritet och teknik. För att minska dessa risker är det bland annat viktigt att göra noggranna riskanalyser, implementera robusta säkerhetsåtgärder, följa upp eventuella leverantörer och ge ett tydligt och tillräckligt omfattande stöd för användarna.

2018 trädde den nya dataskyddsförordningen (GDPR) i kraft. Det främsta syftet med dataskyddsförordningen är skydda människors grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter. Hanteringen av sekretessbelagda uppgifter styrs främst av offentlighets- och sekretesslagen och innebär bland annat att patientuppgifter måste skyddas mot obehörig åtkomst.

Brister i hantering av personuppgifter och skyddet för enskildas integritet 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.

Syfte och revisionsfrågor

Syftet med granskningen är att bedöma om regionstyrelsen har säkerställt att digitala vårdmöten sker på ett ändamålsenligt och lagenligt sätt. Revisionen syftar till att svara på följande frågor:

1. Har ändamålsenlig riskanalys, konsekvensbedömning och lämplighetsbedömning genomförts innan implementering?
2. Finns ändamålsenligt tjänste- och personuppgiftsbiträdesavtal med leverantören av tjänsten?
3. Är de personuppgiftsbehandlingar som digitala vårdmöten innebär, korrekt införda i regionstyrelsens registerförteckning över personuppgiftsbehandlingar?
4. Har tjänsten följts upp på ett ändamålsenligt sätt, avseende skydd av sekretessbelagda uppgifter och personuppgifter?
5. Finns interna regler, rutiner och vägledning som reglerar och stödjer användningen av digitala vårdmöten?

6. Ges patienter och anhöriga information om behandlingen av deras personuppgifter vid de digitala vårdmötena i enlighet med gällande lagstiftning?

Revisionskriterier

- Kommunallag (2017:725)
- Offentlighet- och sekretesslag (2009:400)
- Allmän dataskyddsförordning ((EU) 2016/679) om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter, även kallad GDPR
- Riktlinjer om öppenhet och information till registrerade enligt förordning (EU) 2016/679, WP260rev.01, 2018-04-11.
- Proposition 2022/23:97, Sekretessgenombrott vid utlämnande för teknisk bearbetning eller teknisk lagring av uppgifter
- Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster
- Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster, MSBFS 2018:8
- Vägledning säkerhetsåtgärder i informationssystem, MSB, publikationsnummer MSB2032
- Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården, HSLF-FS 2016:40
- eSams vägledning om utkontraktering: sekretess och dataskydd, 2023-06.

Avgränsning

Granskningen avser möten med patient som sker över video. Regionen kallar den typen av möten för videobesök/besök via video.[1] Inom ramen för denna granskning används dock begreppet digitalt vårdmöte för samma typ av patientmöten.

Granskningsobjekt är regionstyrelsen. Granskningen inriktas i huvudsak till år 2024.

Granskningen har avgränsats till de system/tjänster som används i regionens egna verksamhet (det vill säga privata vårdgivare omfattas inte av granskningen).

Metod

Granskningen har genomförts genom intervjuer och dokumentstudier. Den insamlade dokumentationen har framförallt bestått av dokumenterade riskanalyser och bedömningar, avtal, dokumenterade uppföljningar, interna styrande och stödjande dokument och information avseende digitala vårdmöten som ges till patienter och anhöriga (se Bilaga: Förteckning av granskad dokumentation).

Digitala intervjuer har genomförts med representanter från avdelningen E-hälsa och invånartjänster samt representanter från regionens informationssäkerhetsavdelning. Totalt har digitala intervjuer, möten och telefonsamtal genomförts med sju personer (utöver ovan funktioner även regionens IT-direktör och regionjurist). Information har

[1] Begrepp och formuleringar, Region Hallands vårdgivarwebb (inhämtat mars 2025)

även inhämtats via e-post från samtliga ovan nämnda funktioner samt från representanter vid regionens kommunikationsavdelningen.

De intervjuade har beretts möjlighet att sakgranska rapporten.

Rapporten är kvalitetssäkrad i enlighet med PwCs interna riktlinjer för kvalitetssäkring.

Granskningsresultat

Organisation

Regionkontoret är en del av Region Hallands förvaltning, vars politiska nämnd är regionstyrelsen.[2] Inom Regionkontoret finns verksamhetsområdet IT och digitalisering, vilket har tre områden:

- digitalisering av hälso- och sjukvård,
- digitalisering av stöd och regional utveckling och
- informationsteknologi.

Inom Digitalisering av hälso- och sjukvård finns avdelningen för e-hälsa och invånartjänster, och inom Informationsteknologi finns avdelningen för informationssäkerhet, där dataskyddsenheten ingår. Till Regionkontorets verksamhetsområde tillhör också, bland andra, kommunikationsavdelningen.

Plattformar för digitala vårdmöten

Inom Region Halland genomförs digitala vårdmöten med hjälp av flera olika digitala verktyg. Det framgår av Region Hallands dokument *Rutin: Digital kommunikation med patient* (september 2023) att de plattformar som är godkända för kommunikation med patient via video är Platform24 (Clinic24), HOPE Solution, Microsoft Teams och system som används för MDK.[3] Utöver detta framgår av Region Hallands vårdgivarwebb att även systemet Visiba Care används för kommunikation med patienter via video.[4] Vid intervjuer uppges även att privata vårdgivare tillåts ha egna lösningar[5].

Vid intervjuer beskrivs att de olika tjänsterna används på olika sätt, i olika grad och för olika ändamål. Exempelvis används Teams primärt vid vårdplaneringar mellan regionen, patienten och den kommun som patienten tillhör. Under slutet av granskningen lämnas även uppgift från regionen om att HOPE Solution numera inte används för digitala vårdmöten. Dock är alla fyra ovan nämnda plattformarna godkända för digitala vårdmöten och tillgängliga för den typen av användning.

Nedan följer en beskrivning av de fyra systemen Visiba Care, Platform24, HOPE Solution och Microsoft Teams.

Digitala vårdmöten i Visiba Care

Molntjänsten Visiba Care är en digital plattform för e-hälsolösningar som gör det möjligt för vårdgivare att tillhandahålla rådgivning genom video eller chattmeddelanden online till sina patienter eller klienter. Av intervjuer samt av avtalet mellan leverantören och Region Halland framgår att Visiba Care använts inom regionen sedan början av 2018.

[2] Regionkontorets organisation oktober 2024,
[3] Forum för multidisciplinära diskussioner om diagnostik och behandlingsrekommendationer för cancerpatienter. Utanför ramen av granskningen då systemet används för personal.
[4] Region Hallands vårdgivarwebb: Visiba Care, inhämtat mars 2025.
[5] De privata vårdgivarna är självständigt personuppgiftsansvariga och har därmed ansvaret för de digitala lösningar som de använder.

Systemet levereras som en tjänst och inkluderar licens för programvara, underhåll och support. Tjänsten levereras över internet (vilket innebär att det är en molntjänst).

Digitala vårdmöten i Platform24
Platform24 är ett digitalt vårdstöd som består av två verktyg: Clinic24 och Manage24. Clinic24 är ett verktyg vårdpersonal använder för videobesök och chatt medan Manage24 är ett administratörsverktyg. Region Halland ingick ett avtal avseende plattformen under 2021. Systemet levereras som en webbaserad tjänst i form av ett digitalt vårdstöd och inkluderar licens för programvara, underhåll och support. Tjänsten levereras som en molntjänst.

Digitala vårdmöten i Microsoft Teams
Microsoft Teams används inom regionen för exempelvis vårdplanering. Microsoft Teams är en del av Microsoft 365-paketet och levereras som en molntjänst.

Digitala vårdmöten i HOPE Solution
HOPE Solution är en digital plattform med det avsedda ändamålet att möjliggöra kommunikation mellan patienter och hälso- och sjukvården. Region Halland ingick ett avtal avseende systemet under 2019. Systemet används främst vid regionens barnklinik och lanserades som ett forskningsprojekt i regionen. Ursprungligen var HOPE Solution avsedd att användas inom regionen för datainsamling via patienters mobiltelefoner, men dess användning har utökats till att inkludera digital kommunikation med patienter.

Riskanalys, konsekvensbedömning och lämplighetsbedömning

Revisionsfråga 1: Har ändamålsenlig riskanalys, konsekvensbedömning och lämplighetsbedömning genomförts innan implementering?

Utgångspunkter

Riskanalyser
Riskanalyser avseende informationssäkerhet (och därför också avseende personuppgiftshantering och integritetsskydd) är en process som syftar till att identifiera och hantera potentiella hot och sårbarheter som kan påverka en organisations informationstillgångar. Kravet att genomföra riskanalyser avseende informationssäkerhet framgår av flera lagstiftningar och föreskrifter, bland annat av lag om informationssäkerhet för samhällsviktiga och digitala tjänster[6] samt socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården.[7] Vidare framgår det av MSB:s föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster att en leverantör ska identifiera, analysera och värdera risker för organisationens information, nätverk och informationssystem.[8]

Inför en upphandling eller innan ett system börjar användas behöver en riskanalys genomföras. Syftet är att tydliggöra vilka krav som behöver ställas och att klarlägga vilka

[6] 11-13 §§
[7] 3 kap. 5 §
[8] MSBFS 2018:8, § 8.

säkerhetsåtgärder som behöver vidtas för att uppnå ett adekvat skydd. Om riskanalyser inte genomförs på ett ändamålsenligt sätt kan organisationen misslyckas med att uppfylla sina skyldigheter att skydda informationen, vilket i sin tur kan ge upphov till risker för både organisationen och enskilda individer (primärt patienter och anställda i en hälso- och sjukvårdsverksamhet).

Att genomföra och dokumentera riskanalyser, samt systematiskt arbeta med åtgärdandet av identifierade risker, är också ett sätt att uppfylla principen om ansvarsskyldighet enligt GDPR. Principen innebär att den personuppgiftsansvarige ska kunna visa att behandlingen är förenlig med GDPR och att lämpliga tekniska och organisatoriska åtgärder har vidtagits (i relation till identifierade risker) för att skydda de registrerades rättigheter och friheter (det vill säga kunna visa hur detta går till).

Konsekvensbedömning
Enligt artikel 35.1 i GDPR är den personuppgiftsansvarige skyldig att genomföra en dataskyddskonsekvensbedömning om en behandling sannolikt medför hög risk för individers rättigheter och friheter. Vad som utgör en hög risk kan bedömas med hjälp av den förteckning som är framtagen av Integritetsskyddsmyndigheten (IMY).[9] Exempel på behandlingar med hög risk inkluderar hantering av stora mängder personuppgifter, känsliga personuppgifter (exempelvis hälsouppgifter) eller användning av ny teknik. Syftet med en konsekvensbedömning är att förebygga risker för personlig integritet innan de uppstår. Vanligtvis bör en riskanalys genomföras innan konsekvensbedömningen, för att identifiera eventuella de höga risker som i sin tur konsekvensbedömningen syftar till att analysera och hantera.

Det är den personuppgiftsansvariges ansvar att utföra konsekvensbedömningen, och den bör som regel genomföras innan behandlingen påbörjas. Inom Region Halland är varje styrelse och nämnd personuppgiftsansvarig för de personuppgiftsbehandlingar som sker inom respektive verksamhet. Enligt GDPR ska konsekvensbedömningen minst innehålla en systematisk beskrivning av personuppgiftsbehandlingen, bedömning av behov och proportionalitet, bedömning av riskerna för de registrerades rättigheter och friheter, samt planerade skydds- och säkerhetsåtgärder. Det är också obligatoriskt att konsultera dataskyddsombudet. Om det efter konsekvensbedömningen kvarstår sannolika höga risker, ska IMY kontaktas för förhandssamråd.

Precis som med riskbedömningen behöver konsekvensbedömningen dokumenteras för att principen om ansvarsskyldighet enligt GDPR ska kunna uppfyllas. Att arbeta systematiskt med dokumentation, åtgärdande och uppföljning av konsekvensbedömningar bidrar också generellt till ett systematiskt riskhanteringsarbete som i sin tur ofta bidrar till ökad kvalitet och minskade risknivåer över tid.

Lämplighetsbedömning
När en myndighet outsourcar IT-drift till privata tjänsteleverantörer (vilket som regel är fallet när molntjänster av olika typer används), delas ofta en stor mängd information. En

[9] https://www.imy.se/globalassets/dokument/ovrigt/forteckning---konsekvensbedomningar.pdf, 2025-02-27.

myndighet har det yttersta ansvaret för att säkerställa att informationen hanteras på ett ändamålsenligt sätt och i enlighet med gällande lagar. Enligt 10 kap. 2 a § i offentlighets- och sekretesslagen (OSL) kan sekretessbelagda uppgifter lämnas till en tjänsteleverantör som har i uppdrag att endast tekniskt bearbeta eller lagra uppgifterna, förutsatt att det inte är olämpligt med hänsyn till omständigheterna. Innan uppgifter lämnas ut, måste myndigheten därför göra en lämplighetsbedömning för att säkerställa att utlämnandet sker på ett rättsenligt, säkert och lämpligt sätt.

Till skillnad mot GDPR innehåller inte regeln i OSL något uttryckligt krav på att bedömningen ska dokumenteras eller hur detta ska genomföras. Det framgår av propositionen 2022/23:97, *Sekretessgenombrott vid teknisk bearbetning eller lagring av uppgifter,* att det kan vara lämpligt att den utkontrakterande myndigheten dokumenterar de avvägningar och bedömningar som görs vid ett utlämnande som omfattar en större uppgiftsmängd eller uppgifter som är av känslig karaktär.[10] Vidare framgår av eSams vägledning *Utkontraktering - sekretess och dataskydd* att det är viktigt att den utkontrakterande myndigheten noggrant dokumenterar den utredning och bedömning som myndigheten genomför inför utkontraktering.[11] Det kan vara svårt att göra rätt avvägningar och ett väl underbyggt beslutsunderlag ger en stabil grund för en säker och pålitlig utkontraktering. Det följer även av bestämmelsen i GDPR att bedömningen behöver vara genomförd innan en utlämning sker (exempelvis när en tjänst för videomöten börjar användas), eftersom frågan om utlämningen är lagenlig eller ej är ett resultat av själva bedömningen. Mot bakgrund av detta är det idag relativt vanligt förekommande att särskilda dokument/formulär används för att underlätta genomförandet av lämplighetsbedömningen.

Iakttagelser

Riskanalyser och bedömningar

Visiba Care

Under granskningen har vi inte kunnat identifiera varken någon dokumenterad riskanalys, konsekvensbedömning eller lämplighetsbedömning som avser användningen av Visiba Care från införandet av systemet 2017 fram till 2025.

Det framgår av huvudavtalet mellan leverantören och Region Halland att detta avtal med Visiba Care tecknades under 2017, det vill säga innan GDPR trädde i kraft. Vid intervjuer uppges detta vara skälet till att analys och bedömningar inte är genomförda. Däremot beskrivs att det inför driftsättningen av Visiba Care genomfördes ett omfattande förarbete som inkluderade bland annat riskkartläggning, genomlysning av leverantören och planering för uppsättning av tjänsten hos regionen. Dock har vi inte kunnat ta del av någon dokumentation från det beskrivna förberedelsearbetet.

Under början av 2025 tecknades ett nytt avtal avseende Visiba Care (se revisionsfråga 2). Under granskningen har vi tagit del av ett utkast till en konsekvensbedömning av

[10] Proposition 2022/23:97 s.17.

[11] eSAMs vägledning Utkontraktering - sekretess och dataskydd s.28

systemet, vilket också innehåller en riskanalys (februari 2025). Utkastet avser användningen av Visiba Care från och med 2025.

Riskanalysen tar upp typiskt förekommande risker för den aktuella behandlingen. Skattningen av flera konsekvenser är låg (exempelvis riskvärde 2 av 4 avseende att sekretessbelagda uppgifter röjs, eller att personuppgifter inte är tillgängliga i vården när de behövs). Detta får till följd att flera risker sammanvägt bedöms som låga, och därmed behöver inte risksänkande åtgärder vidtas.

Konsekvensbedömningen för samma system är påbörjad men ett antal betydande frågor och osäkerheter kvarstår att komplettera bedömningen med. Avseende lämplighetsbedömningen kan vi inte se att konsekvensbedömningen adresserar den frågan, eller att den dokumenteras på ett annat sätt.

I februari 2025 fattades beslut av förvaltningschef/sjukhuschef om att påbörja behandlingen av personuppgifter innan konsekvensbedömningen blivit färdigställd.

Microsoft Teams
Under granskningen har vi inte kunnat identifiera varken någon dokumenterad riskanalys, konsekvensbedömning eller lämplighetsbedömning.

Vid intervjuer uppges att det påbörjats en övergripande riskanalys för användningen av Microsofts tjänster inom regionen, men att denna inte blivit färdigställd. Under granskningen har vi även tagit del av riskanalys (odaterad men sannolikt genomförd under 2020) och delrapport (2021) avseende övergången till Microsoft 365 för administrativa tjänster. Vi har även tagit del av en konsekvensbedömning för samverkan i molnet för analys av vårdrelaterad data (2024).

Platform24
Under granskningen har vi tagit emot utkast till riskanalys och konsekvensbedömning, dels en version daterad september 2022, och dels en odaterad som uppges vara en uppdaterad version. Båda versionerna är utkast med relativt lite information. Vi har inte mottagit någon lämplighetsbedömning (varken självständigt dokument eller integrerat i konsekvensbedömning).

Vid intervjuer uppges att den första versionen av konsekvensbedömningen för Platform24 påbörjades inför lanseringen under 2021. Utkastet kunde inte färdigställas eftersom information från leverantören och olika tekniska lösningar vid upprepade tillfällen förändrades. Det andra utkastet vi tagit del av (det odaterade dokumentet) beskrivs under intervjuer vara en påbörjad konsekvensbedömning som bättre ska spegla den nuvarande situationen.

HOPE
Vi har tagit del av *Konsekvensbedömning avseende dataskydd, HOPE Solution* (fastställd januari 2019) vilken innehåller en konsekvensbedömning och en riskanalys av systemet. Konsekvensbedömning avser dock inte digitala vårdmöten, och den personuppgiftsbehandling som det innebär, utan ett pilotprojekt där systemet skulle

användas för överföring av vissa hälsouppgifter genom en app mellan patient och vårdgivare. I övrigt har vi inte kunnat identifiera dokumenterad riskanalys eller lämplighetsbedömning.

Övrig dokumentation

Det framgår av *Rutin: Digital kommunikation med patient* (februari 2022) att de system som Region Halland använder för att kommunicera digitalt med patienter är säkerhetskontrollerade innan de införs i verksamheten för att vårdpersonalen ska vara trygg i att använda systemen. Vidare framgår av *Rutin: Distanskontakt - tillämpningsanvisning* (februari 2022) att införandet av nya digitala tjänster och tekniska plattformar alltid ska hanteras utifrån ett patient- och informationssäkerhetsperspektiv och följa gällande lagar, förordningar och föreskrifter. Vidare framgår att vårdgivaren ska identifiera de risker som uppstår för patienter och verksamheter när ny eller förändrad teknik, arbetssätt, metod eller processer införs. Riskanalysen ska dokumenteras och i dokumentationen ska det framgå vilka skyddsåtgärder som har implementerats för att helt undvika och/eller minimera identifierade risker. Enligt rutinen ska särskild försiktighet iakttas gällande molntjänster.

Regionen har en fastställd rutin som beskriver hur konsekvensbedömning avseende dataskydd ska genomföras, *Rutin: Konsekvensbedömning avseende dataskydd (DPIA)* (januari 2022), med tillhörande blankett *Blankett: Konsekvensbedömning avseende dataskydd (DPIA) - enligt artikel 35 GDPR.* Blanketten för konsekvensbedömningen innehåller dessutom instruktioner för genomförandet av en riskanalys. Rutinen utgår från regional riktlinje för informationssäkerhet och dataskydd och är just nu under uppdatering då vissa delar behöver förbättras, enligt skriftlig återkoppling från regionen.

Det framgår av *Riktlinje 309 Informationssäkerhet RH* (december 2022) att avtal med en molntjänstleverantör inte får tecknas innan en riskanalys genomförts och det finns beslut på om tjänsten får användas.

Av Region Hallands riktlinje *Säkerhet - Riktlinjer för Informationssäkerhet och dataskydd* (juni 2020) framgår att konsekvensbedömningar avseende dataskydd regelbundet ska redovisas.

Vidare finns en checklista för vilka åtgärder och bedömningar som ska genomföras vid upphandling av nya IT-system, *Instruktion: Informationssäkerhetskrav - vårdrelaterade informationssystem* (juli 2022). Ett av de moment som behöver checkas av enligt den instruktionen är genomförande av en konsekvensbedömning. Vid intervjuer beskrivs att rutinerna är kommunicerade i organisationen men att de inte är obligatoriska att följa.

Intervjuer

Under intervjuer beskrivs vidare att avsaknaden av genomförda risk-, konsekvens- och lämplighetsbedömningar beror på flera omständigheter. En orsak är att tjänsterna är upphandlade innan GDPR och förändringen i OSL trädde i kraft. Det beskrivs även att upphandling och införande av nya system har prioriterats. Det beskrivs även att en

generell tidsbrist gör det svårt att genomföra analyserna och bedömningarna men det poängteras att utkast i vissa fall har påbörjats.

Vid intervjuer samt vid skriftlig återkoppling från regionen beskrivs att det är verksamheten som ansvarar för den planerade personuppgiftsbehandlingen som även är ansvarig för att en konsekvensbedömning genomförs samt godkänns. Ansvarig för detta kan vara projektägare, förvaltningschef, verksamhetschef eller motsvarande och genomförs på uppdrag av personuppgiftsansvarig. Av uppgifter från regionen framgår att ansvarig för att konsekvensbedömningen aktualiseras och följs upp med jämna mellanrum är den verksamhet som ansvarar för att konsekvensbedömningen genomförs. Det ska ske i dialog med dataskyddsenheten.

Vidare beskrivs att avdelningen för informationssäkerhet och dataskyddsenheten inte alltid involveras vid anskaffning av IT-tjänster och applikationer. En process för att utveckla en checklista som omfattar hela upphandlingsprocessen är för närvarande under utveckling, för att bland annat ge bättre förutsättningar för kvalitetssäkring i ett tidigare skede.

Avseende avsaknaden av lämplighetsbedömningar beskrivs vid intervjuer och i skriftlig återkoppling från regionen att det i dagsläget inte finns någon rutin fastställd för detta arbete. Det framhålls även att lämplighetsbedömning har efterfrågats från regionjuristerna, när det har bedömts nödvändig. Vid de första intervjuerna med regionen framkom att kravet på att genomföra lämplighetsbedömningar vid utkontraktering av IT-drift var relativt okänt. Under granskningens gång framkom dock att regionen inte använder begreppet “lämplighetsbedömning” och att regionen gjort tolkningen att dessa bedömningar inte behöver dokumenteras.. Intervjuade beskriver att resonemang som är relevanta vid utkontraktering av IT-drift har förts muntligt, men att dessa resonemang inte har dokumenterats. Det framförs även att man utifrån hur den aktuella lagparagrafen är skriven, inte behöver dokumentera lämplighetsbedömningen.

Bedömning

Har ändamålsenlig riskanalys, konsekvensbedömning och lämplighetsbedömning genomförts innan implementering?

Nej.

Granskningen visar att regionen inte har genomfört och dokumenterat varken riskanalys, konsekvensbedömning eller lämplighetsbedömning, på ett fullständigt sätt för någon av de tjänster som är godkända att använda för digitala vårdmöten. Det är dock tydligt att diskussioner avseende frågeställningarna har förts.

Avseende HOPE, Teams och Visiba Care fram till och med 2024, bedömer vi att avseende användning av dessa för digitala vårdmöten har det inte genomförts varken riskanalys, konsekvensbedömning eller lämplighetsbedömning. Avseende Platform24 finns visserligen utkast till konsekvensbedömningar, men de är så pass ofullständiga att bedömning inte kan göras.

Vi bedömer att den riskanalys som finns avseende Visiba Care, avseende användning från 2025, tar upp de flesta typiskt förekommande risker. Dock är skattningen av flera

konsekvenser satt anmärkningsvärt lågt. Att skatta risker för lågt kan innebära en risk för att riskreducerande åtgärder inte vidtas, och därmed kvarstår eventuella risker för patienter och övriga användare av systemet. Avseende konsekvensbedömningen för samma system är denna i allt väsentligt i enlighet med kraven i GDPR, men ett antal betydande frågor och osäkerheter kvarstår att komplettera bedömningen med. Vi kan heller inte se att någon lämplighetsbedömning är genomförd avseende den förnyade användningen av Visiba Care.

Avseende frågan om lämplighetsbedömningen behöver dokumenteras, och hur detta behöver ske, bedömer vi att det är relativt tydligt (genom både lagkrav, förarbeten och vägledning) att någon form av dokumentation behöver ske, bland annat för att det ska vara möjligt att visa att övervägandet har genomförts innan utlämning påbörjats. Däremot behöver inte dokumenationen vara i form av ett självständigt dokument, utan skulle exempelvis kunna göras som en integrerad del av konsekvensbedömningen. Detta kan vi dock inte se har skett i något fall inom ramen för denna granskning.

Både lagstiftning och interna styrande dokument ställer relativt tydliga krav på att samtliga tre analyser och bedömningar behöver göras innan de aktuella tjänsterna används. Konsekvensbedömning enligt GDPR och lämplighetsbedömning enligt OSL är inte tvingande för användning av alla typer av IT-tjänster, men vid användning där patientuppgifter förekommer och där den tekniska lösningen innebär en molntjänst är det osannolikt att det inte behövs. Inom ramen för denna granskning har vi heller inte mottagit resonemang eller bedömningar avseende att analys och bedömningarna inte behövs, utan endast att de till största del inte är genomförda.

Avseende faktumet att några av tjänsterna började användas innan de aktuella reglerna trädde i kraft är inte relevant eftersom reglerna gäller all pågående användning, oavsett när den påbörjades.

Vi noterar att det finns etablerade rutiner och blanketter som stöd för att genomföra bedömningar, vilket är positivt. Uppenbarligen brister dock efterlevnaden och användningen av dessa.

Sammantaget innebär detta en betydande risk för att regionen inte har kontroll på de informationssäkerhets- och integritetsskyddsrisker som användningen av de aktuella tjänsterna för med sig och att adekvata säkerhetsåtgärder därmed inte är implementerade. Risken är även betydande för att varken GDPR eller OSL efterlevs. I och med att det finns en betydande risk för att kontroll avseende risker och behov av säkerhetsåtgärder saknas, finns även en risk för att sekretessbelagda uppgifter röjs.

Tjänste- och personuppgiftsbiträdesavtal

Revisionsfråga 2: Finns ändamålsenligt tjänste- och personuppgiftsbiträdesavtal med leverantören av tjänsten?

Utgångspunkter

Det som styr om villkoren i avtalet är ändamålsenliga eller ej, är i vilken grad de tillförsäkrar regionen att de lagar och regler som gäller för regionen kan efterlevas även om en tjänst, i detta fall en digital mötestjänst, tillhandahålls av en extern part. Det kan

handla om villkor av formell karaktär, men det kan också handla om kommersiella villkor som är avsedda att skapa bästa möjliga förutsättningar för att avtalet ska följas och hur olika typer av situationer som kan uppstå ska lösas (exempelvis om leverantören inte kan leverera som planerat).

När det gäller PUB-avtalet är det obligatoriskt enligt GDPR[12] när personuppgifter ska behandlas på uppdrag av en personuppgiftsansvarig (PUA). PUA behöver, både genom kravställning i upphandlingen och genom villkor i huvudavtal/tjänsteavtal och PUB-avtalet, förvissa sig om att personuppgiftsbiträdet (PUB) kan behandla personuppgifterna på ett sätt som är lagenligt och ger ett tillräckligt skydd för den enskildes personuppgifter. Utöver det behöver själva PUB-avtalet innehålla ett antal obligatoriska villkor och instruktioner, exempelvis vilka personuppgifter som får behandlas, hur länge de får behandlas och hur personuppgifter ska skyddas för att få ett fullgott skydd. Instruktionerna behöver vara relativt specifika och avgränsade. Syftet med detta är att den personuppgiftsansvariga (regionen i detta fall) ska kunna behålla kontrollen över personuppgiftsbehandlingen.

Iakttagelser

Avtalsgranskning

Nedan följer en översiktlig genomgång av de tjänste- och PUB-avtal (inklusive eventuella bilagor) som har tillhandahållits inom ramen för denna granskning.

Visiba Care

Under granskningen har vi tagit del av det tjänsteavtal som tecknats mellan Region Halland och Atea Sverige AB i november 2017. Tjänsteavtalet innehåller även ett licensavtal mellan Region Halland och Visiba Group AB. Vi har även tagit del av *Personuppgiftsbiträdesavtal mellan personuppgiftsansvarig och personuppgiftsbiträde avseende molntjänsten Visiba Care*, signerad mars-juni 2018), samt *Instruktioner vid behandling av personuppgifter för Region Halland* (odaterad), vilket, utgör en integrerad del av PUB-avtalet avseende molntjänsten Visiba Care. Granskningen har även tagit del av en lista avseende de underbiträden som anlitats för behandling av personuppgifter under PUB-avtalet avseende Visiba Care, *Bilaga B: Lista över underbiträden* (undertecknad april 2021).

Avtalet är från 2017 och de bilagor avseende personuppgiftsbehandling och dataskydd följer inte de krav som gäller i idag i och med att GDPR började gälla 2018. Som ett tilläggsavtal finns PUB-avtalet med Visiba Group, som tecknades 2018 och i vissa avseenden har uppdaterats sedan dess. Utifrån det material vi haft tillgängligt under granskningen framgår inte den avtalsrättsliga kopplingen mellan tjänste-/huvudavtalet med Atea och PUB-avtalet med Visiba Group.

Tjänsteavtalet saknar villkor avseende sekretess eller informationssäkerhet. Personuppgiftbiträdesavtalet följer i allt väsentligt kraven i GDPR, och går till viss del även utöver dessa. Det framgår av PUB-avtalet att leverantören ska vidta alla lämpliga

[12] GDPR art 28.

säkerhetsåtgärder för att skydda personuppgifterna som behandlas. Dock saknas mer specifika instruktioner från regionen till leverantören avseende vilka dessa åtgärder bör vara. Av PUB-avtalet framgår krav på att leverantörens medarbetare och anlitade konsulter ska ingå sekretessavtal och/eller upplysas om att tystnadsplikt föreligger (avseende den information och personuppgifter från Region Halland som de kan behöva ta del av genom sitt arbete).

Från 2025 finns ett nytt avtal för Visiba Care som vi också har tagit del av. Strukturen på detta avtal är i allt väsentligt densamma, dock med ett uppdaterat innehåll (främst i relation till GDPR). Även i detta avtal saknas villkor i tjänsteavtalet med Atea avseende informationssäkerhet, dataskydd och sekretess. Det beskrivs i tjänsteavtalet att Atea anlitar en underleverantör (Visiba Group) för avtalets fullgörande och att Atea ansvarar för underleverantören. Samtidigt biläggs även generella användarvillkor för Visiba Group till tjänsteavtalet. Där beskrivs att det finns ytterligare ett avtal som reglerar relationen mellan Atea och Visiba Group, avseende leveransen till kunden (regionen). Detta avtal benämns som underleverantörsavtal, men biläggs inte avtalet mellan Atea och Region Halland. I användarvillkoren bekräftas att Visiba Group är en underleverantör till Atea. Det framgår också att i det fall det skulle finnas motsägelser mellan olika dokument inom avtalet och dess bilagor, ska de allmänna användarvillkoren gälla i första hand. Användarvillkoren innehåller också en begränsning av rätten att väcka skadeståndsanspråk, nämligen en tidsfrist om 90 dagar.

Trots att Visiba Group benämns som underleverantör finns inget PUB-avtal med Atea, utan endast med Visiba Group. Detta upplägg följer samma upplägg som för det äldre avtalet avseende Visiba Care.

Platform24
Vi har tagit del av det avtal som tecknades mellan Region Halland och Atea Sverige AB i september 2021, *Leverans från Licenspartneravtal mellan Region Halland och Atea Sverige AB*, *avseende Platform24*. Avtalet avser både licenser för Platform24 och tjänsten leverans av den digitala plattformen (systemet). Avtalet innehåller inga villkor avseende sekretess eller informationssäkerhet.

Under granskningen har vi även tagit del av *Personuppgiftsbiträdesavtal, Platform24 Healthcare AB* (signerad september-oktober 2021), inklusive instruktioner för behandling av personuppgifter samt en lista över underbiträden. PUB-avtalet är tecknat mellan Region Halland och Platform 24 Healthcare AB. I avtalet refereras till “huvudavtalet” som definieras som det avtal där det aktuella PUB-avtalet är en bilaga till. Det är dock oklart vilket avtal som avses eftersom PUB-avtalet inte är en bilaga till licens- och tjänsteavtalet. De båda avtalen (huvud- respektive PUB-avtal) har också ingåtts med olika parter (Atea respektive Platform24 Healthcare AB).

PUB-avtalet följer i allt väsentligt kraven i GDPR och det mallavtal som SKR har tagit fram.

HOPE Solution
Vi har tagit del av det avtal som tecknades mellan Region Halland och leverantören Addi Medical i juni 2019, *Prenumerationsvillkor för HOPE Solution*. Avtalet innehåller inga villkor avseende sekretess eller informationssäkerhet.

Under granskningen har vi även tagit del av *Personuppgiftsbiträdesavtal Addi Medical AB (HOPE Solution)* (signerat i december 2022), inklusive instruktioner för behandlingen och en lista över underbiträden. Avtalet följer i allt väsentligt kraven i GDPR och det mallavtal som SKR har tagit fram. Av PUB-avtalet framgår krav på att leverantörens medarbetare och anlitade konsulter ska ingå sekretessavtal och/eller upplysas om att tystnadsplikt föreligger (avseende den information och personuppgifter från Region Halland som de kan behöva ta del av genom sitt arbete). Det innehåller även en specificerad instruktion som bland annat beskriver vilka uppgifter som får behandlas, för vilket ändamål och vilka säkerhetsåtgärder som minst behöver vidtas.

Det framgår i avtalet att leverantören inte har några underleverantörer.

Behandlingen av personuppgifter kommer, enligt PUB-avtalet, att utföras på utrustning som befinner sig i EU/EES eftersom HOPE Solution fortsätter driftas av personuppgiftsansvarig. Det framkommer att insamlade personuppgifter överförs till och lagras i personuppgiftsbiträdets IT-system. Supportfunktionen kan, efter PUA godkännande, erhålla åtkomst till HOPE-plattformens miljö vid regionen, vilken kan medföra tillgång till patientuppgifter. Enligt instruktionerna får dessa inte flyttas till någon annan miljö. Det framkommer vidare att PUB lagrar supportärenden via Dropbox, vilket innebär en tredjelandsöverföring. Supportärendena får dock inte innehålla personuppgifter, varken för regionens anställda eller för patienter. Det framgår inte om det finns tekniska säkerhetsåtgärder som hindrar överföring av uppgifter från regionens miljö till leverantörens miljö, samt överföring av personuppgifter till Dropbox.

Microsoft Teams
Under granskningen har vi tagit del av de användarvillkor avseende användning av Microsofts tjänster (som är relevanta för denna granskning); *Microsofts molntjänster & svenska krav på integritet och patientdatasäkerhet* (2017), *Villkor för Onlinetjänster* (januari 2016) och Dataskyddstillägg för Microsofts professionella tjänster (september 2022).

Användarvillkoren är standardvillkor som gäller för de flesta kunder inom Sverige och EU. Därför är de skrivna utifrån ett övergripande perspektiv och är inte specifika för användning av Teams för digitala vårdmöten. Villkoren kan även generellt ensidigt ändras av Microsoft. I samtliga villkor finns ett generellt åtagande för Microsoft att följa tillämplig lagstiftning, och dataskyddstillägget uppfyller kravet på PUB-avtal enligt GDPR.

Övrig dokumentation
Granskningen har även tagit del av *Rutin: Personuppgiftsbiträdesavtal (PUB-avtal) i upphandlingar* (oktober 2022) vars syfte är att beskriva arbetsprocessen för att

identifiera vilka av regionens upphandlingar som kräver PUB-avtal och att beskriva den praktiska hanteringen för dessa upphandlingar. Rutinen beskriver att om upphandlarens initiala bedömning tyder på att ett PUB-avtal krävs, ska upphandlaren kontakta dataskyddsenheten och kontrollera att förfrågningsunderlaget gentemot leverantör innehåller krav om att anbudsgivaren accepterar regionens mall för PUB-avtal. Mallen utgår från Sveriges Kommuner och Regioners framtagna mall och har kompletterats med ytterligare säkerhetsinstruktioner framtagen av regionen. Vidare beskrivs att upphandlaren ska kontakta dataskyddsenheten inför annonsering och i samband med tilldelningen och rutinen innehåller även ett förslag till formulering för kravet vid upphandling avseende PUB-avtal. Vid upphörande av avtal ska återigen upphandlaren kontakta dataskyddsenheten.

Intervjuer

Vid intervjuer beskrivs att det är avdelningen för informationssäkerhet som ansvarar för att ta fram och hantera PUB-avtal. De sköter det praktiska arbetet, har kontakt med leverantörer och för diskussioner inom verksamheten. Det uppges att generellt används SKR:s mallar.

Avseende Platform24 beskrivs vid intervjuer att både tjänsteavtal och PUB-avtal är under uppdatering.

Vid sakgranskning framkommer vidare att regionen utifrån en egen bedömning och diskussion med leverantören Atea, valt upplägget att ha licens-/tjänsteavtal med Atea, och PUB-avtalet direkt med deras underleverantör (i dessa fall Visiba Care och Platform24). Valet har gjorts utifrån att man anser att leverantören egentligen inte behandlar några personuppgifter, utan det sker endast hos underleverantören.

Bedömning

Finns ändamålsenligt tjänste- och personuppgiftsbiträdesavtal med leverantören av tjänsten?

Delvis.

Det är positivt att det finns aktuella tjänsteavtal och PUB-avtal för samtliga tjänster. Det är också positivt att det finns en rutin som tydligt beskriver processen för arbetet, de olika funktionernas roller och ansvar samt konkret stöd genom exempelvis kravformulering.

Avseende de granskade avtalen är alla dessa äldre än rutinen och flera av dem tecknades under de första åren som GDPR gällde. Generellt var både regioner (kunder) och leverantörerna inledningsvis relativt omogna i sitt arbete avseende främst PUB-avtalens utformning, vilket också avspeglas i de granskade avtalen.

PUB-avtalen för Platform24, Hope Solution och det nya PUB-avtalet för Visiba Care bedöms vara väl utformade och innehåller den grad av specificering som är nödvändig för att ett ändamålsenligt skydd för uppgifterna ska kunna uppnås.

Avseende Visiba Care och Platform24 är det problematiskt att den leverantör som är kontrakterad för licenser och och tjänst inte är densamma som PUB-avtal ingåtts med. Tjänsteavtalen innehåller inga villkor avseende sekretess, informationssäkerhet eller dataskydd. Det gör däremot PUB-avtalen. Men eftersom dessa är tecknade med en annan part, som inte är avtalsmässigt knuten till (exempelvis genom att de olika avtalen är bilagor till varandra) tjänsteleveransen uppstår en risk för svårigheter att på ett effektivt sätt utkräva ansvar av leverantörerna, vilket i sin tur innebär en risk för ett svagare skydd för de behandlade personuppgifterna.

De nya avtalen avseende Visiba Care (med Atea respektive Visiba Group) innehåller flera villkor och skrivningar som kan innebära att skyddet för personuppgifter försämras. Exempelvis är det olämpligt med en tidsgräns om 90 dagar för skadeståndsanspråk eftersom det inte är säkert att en incident och/eller skada upptäcks inom den tidsramen. Innehållet i de olika dokumenten som ingår i avtalen, i kombination med att de är tecknade med olika parter och saknar en avtalsmässig koppling till varandra, gör även att regleringen av tjänsten Visiba Care är svårtolkad och därmed oförutsägbar.

Vi förstår till viss del hur regionen har resonerat när valet av avtalsupplägg gjorts. Dock är vår bedömning att det skapar onödiga risker för både regionen och skyddet för personuppgifterna. Vår bedömning är att liknande köp av samma typ av tjänster/system kan regleras på ett tydligare sätt och som inkluderar ett bättre skydd för den information som systemen behandlar. Exempelvis kan avtalen knytas till varandra genom att vara bilagor till varandra och villkor om tolkningsordning av dokument (utifrån att de olika avtalen behöver tillämpas tillsammans för ett effektivt skydd och ansvarsutkrävande).

Registerförteckning

Revisionsfråga 3: Är de personuppgiftsbehandlingar som digitala vårdmöten innebär, korrekt införda i regionstyrelsens registerförteckning över personuppgiftsbehandlingar?

Utgångspunkter

Av artikel 30 i GDPR framgår att personuppgiftsansvarige är skyldig att föra ett register över sina behandlingar av personuppgifter. Genom registret får organisationen en tydlig översikt över vilka personuppgifter som behandlas, hur de används och av vilka parter. Detta underlättar för organisationen att ha kontroll över sina behandlingarna och att identifiera eventuella risker och brister.

Registret över personuppgiftsbehandlingar ska upprättas skriftligen, vara tillgängligt i elektroniskt format och hållas uppdaterade.[13] Av artikel 30 i GDPR framgår att registret ska innehålla namn och kontaktuppgifter för den personuppgiftsansvariga, den personuppgiftsansvariges företrädare samt dataskyddsombudet, ändamålen med behandlingen, en beskrivning av kategorierna av registrerade och kategorierna av personuppgifter och de kategorier av mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut. I tillämpliga fall ska registret även innehålla information om att

[13] IMY, Det här gäller enligt dataskyddsförordningen: Föra register över behandling (inhämtat februari 2025).

överföringar av personuppgifter sker till ett tredjeland. Om möjligt ska registret även innehålla de förutsedda tidsfristerna för radering av de olika kategorierna av uppgifter samt en allmän beskrivning av tekniska och organisatoriska säkerhetsåtgärder.

Iakttagelser

Granskad dokumentation

Granskningen har tagit del av skärmklipp och skärmdelning av regionens register över personuppgiftsbehandlingar. De fyra system som används för digitala vårdmöten via video återfinns i registerförteckningen. I registret finns information om systemets namn och dess ändamål, information om vem som är personuppgiftsbiträde, länk till PUB-avtal, systemets registertyp (exempelvis vårdregister och kommunikation), systemets huvudkategori (exempelvis vårdadministration och personal), vilka som är personuppgiftsansvariga, kategori av registrerade (exempelvis patienter och personal) och kategori av uppgifter (exempelvis personnummer, födelsedatum och telefonnummer) samt information om hur ofta registret gallras. Vidare framgår av registret om och var uppgifter lämnas ut (inom Sverige, inom EU/EES eller till tredje land), status för detta och till vem informationen lämnas ut. Slutligen innehåller registret information om vidtagna säkerhetsåtgärder och eventuella kommentarer.

Alla fyra systemen som används för digitala vårdmöten finns med i registerförteckningen. Däremot är registret inte helt komplett ifyllt för alla systemen. Exempelvis uppges inte att patienters personuppgifter behandlas i Teams, kategorin närstående saknas för flera av systemen (uppgifter om närstående kan behandlas utifrån att detta kan komma upp i samtal med patienten), och för vissa av systemen saknas uppgift om att de används för just digitala/videomöten.

Det är också oklart hur uppdaterat registret är avseende de fyra systemen. Dels utifrån att det för Platform24 anges att förteckningen ska uppdateras när anmälan om behandling inkommer från verksamheten (behandlingen har pågått sedan åtminstone 2021), och dels eftersom det utifrån de saknade uppgifterna framstår som att uppgifterna inte riktigt speglar den aktuella användningen. Vid sakgranskningen förtydligar regionen att kommentaren i registerförteckningen grundar sig i att Platform24 genomgår en uppdatering, vilket innebär att uppgifterna kommer att uppdateras.

Intervjuer

Under intervjuer framkommer att avdelningen för informationssäkerhet har tillgång till registerförteckningen över personuppgiftsbehandlingar och ansvarar för införande och ändringar av behandlingar. När nya system införs eller uppdateringar sker, läggs dessa till i registerförteckningen, och när det är känt att ett system inte längre används, avslutas det. Informationen om sådana förändringar kommer ibland från verksamheten, och uppdateringar av förteckningen görs baserat på den information som informationssäkerhetensavdelningen erhåller. Därför är förteckningens omfattning, aktualitet och korrekthet beroende av att informationssäkerhetsavdelningen får information om förändringar.

Vidare uppges att informationssäkerhetsavdelningen årligen ska kontakta alla regionens förvaltningar med syfte att uppdatera registerförteckningen, och att detta arbete är en del av avdelningens årshjul av återkommande aktiviteter. Vid intervjuer framkommer att detta dock inte alltid görs årligen. Uppdateringar kan då istället ske utifrån behov från verksamhet eller vetskap om förändringar.

Bedömning

Är de personuppgiftsbehandlingar som digitala vårdmöten innebär, korrekt införda i regionstyrelsens registerförteckning över personuppgiftsbehandlingar?

Delvis.

På övergripande nivå uppfyller registerförteckningen kraven i GDPR. Förteckningen har dessutom kompletterats med visst innehåll, exempelvis länk till PUB-avtal, vilket är positivt eftersom det gör registret till ett mer praktiskt och användningsbart verktyg. Vi bedömer dock att det är en brist att registerförteckningen inte är fullständigt ifyllt för alla fyra system och att det inte framgår tydligt om och när registret är uppdaterat.

Risken med att inte ha ett korrekt och uppdaterat register är att det gör det betydligt svårare att ha kontroll över vilka personuppgifter som regionen behandlar och ansvarar för. Bristen på kontroll gör det i sin tur svårare att överblicka risker och behov av säkerhetsåtgärder, vilket ökar risken för säkerhetsbrister och felaktiga prioriteringar.

Uppföljning

Revisionsfråga 4: Har tjänsterna följts upp på ett ändamålsenligt sätt, avseende skydd av sekretessbelagda uppgifter och personuppgifter?

Utgångspunkter

Uppföljning på olika sätt är nödvändigt för att säkerställa att Region Halland följer både de lagar, regler och riktlinjer som gäller för hantering av personuppgifter och sekretesskyddad information. När verksamhet bedrivs genom eller med hjälp av externa parter, exempelvis en leverantör, behöver uppföljning ske för att säkerställa att villkoren i avtalen följs.

Lagkrav avseende uppföljning finns både direkt och indirekt. Exempel på ett direkt krav är det som finns i lag om informationssäkerhet i samhällsviktiga och digitala tjänster där krav på en årlig, övergripande uppföljning finns.[14] Krav på uppföljning framgår även av GDPR. Den personuppgiftsansvarige får endast anlita biträden som ger “tillräckliga garantier” för att den enskildes integritet skyddas.[15] Europeiska dataskyddsstyrelsen har, i vägledning för hur kravet ska tolkas, uttalat att detta är en kontinuerlig förpliktelse som behöver följas upp av den personuppgiftsansvarige, genom exempelvis revisioner och inspektioner.[16] Det följer även av OSL att utlämnande av sekretessbelagda uppgifter (som ofta är fallet vid användning av molntjänst) bland annat behöver grunda sig på en

[14] 3 kap. 6 §
[15] GDPR art. 28.
[16] Riktlinjer 07/2020 angående begreppen personuppgiftsansvarig och personuppgiftsbiträde i GDPR Version 2.0, p. 99.

lämplighetsbedömning, som i sin tur påverkas av aktuella förhållanden.[17] Det innebär i sin tur att uppföljning behöver ske för att säkerställa om de förhållanden som den initiala lämplighetsbedömningen grundade sig på fortfarande gäller. Exempel på ett indirekt krav är regeln i kommunallagen om att nämnden ska se till att verksamheten följer gällande regler och ha en tillräcklig intern kontroll. För att efterleva dessa krav i praktiken är uppföljning nödvändig.[18]

Att genomföra kontinuerlig uppföljning är således avgörande både för att minimera risker och säkerställa att systemet är tillräckligt säkert, men också för att skydda enskildas integritet i enlighet med gällande lagkrav.

Iakttagelser

Avtal

Platform24 och HOPE Solution

PUB-avtalen för HOPE Solution och Platform24 följer samma mall och har liknande formuleringar avseende uppföljning. I båda PUB-avtalen mellan leverantörerna och regionen framkommer att personuppgiftsbiträdena minst en gång om året ska granska säkerheten avseende personuppgiftsbehandlingen genom en egenkontroll för att säkerställa att behandlingen följer PUB-avtalet. Resultatet av den egenkontrollen ska på begäran lämnas till regionen.

Personuppgiftsbiträdet ska också, utan onödigt dröjsmål, kunna redogöra för vilka tekniska och organisatoriska säkerhetsåtgärder som används inom ramen för avtalet. Utöver detta får även regionen, själv eller genom annan, följa upp att PUB-avtalet uppfyller PUB-avtalets, instruktionens och dataskyddslagstiftningens krav.

Visiba Care

Genom villkor i personuppgitsbiträdesavtalet ges regionen möjlighet att genomföra uppföljning av leverantören. Av avtalet framgår att personuppgiftsansvarig har rätt att själv eller genom tredje man få tillgång till anläggningar, information och register för att kunna kontrollera att personuppgiftsbiträdet samt eventuella underbiträden uppfyller de åtaganden som har beskrivits i biträdesavtal.

Microsoft Teams

Enligt PUB-avtalet har regionen möjlighet att följa upp hur Microsoft hanterar personuppgifter i den aktuella tjänsten. Enligt avtalet ska Microsoft själva genomföra granskningar årligen, och rapporterna över dessa granskningar tillhandahålls kunden på begäran. Även mer omfattande revision initierad av kunden är enligt avtalet möjlig.

Övrig dokumentation

Under 2019 genomfördes uppföljning av flera leverantörer där Visiba Group AB var en av dessa. Granskningen utgjordes av ett frågeformulär där leverantören svarade på ett antal frågor avseende bland annat fysisk säkerhet, arbetsmetoder och rutiner avseende

[17] Proposition 2022/23:97, s. 13.
[18] 6 kap. 6 §

hantering av hårdvara, behörighetskontroll, nätverkssäkerhet, säkerhetskopior, incidenthantering och dokumentation. Inom ramen för granskningen granskades även leverantörens personuppgiftsbiträdesavtal med underbiträden. Utfallet av granskningen var tillfredsställande eftersom leverantören hade implementerat ändamålsenliga säkerhetsåtgärder och säkerställt tillräcklig avtalsreglering med underbiträdena.

Under 2021 genomfördes en genomlysning av samtliga tecknade PUB-avtal avseende personuppgiftsbiträden och dess underbiträden. Vi har tagit del av det presentationsunderlag som användes vid presentationen av utfallet, *Utredning gällande överföring av personuppgifter till tredje land* (april 2021). Bakgrunden till utredningen var den dom i EU-domstolen som ändrade förutsättningarna för överföring av personuppgifter till USA, och generellt gjorde dessa överföringar mer komplicerade och rättsligt osäkra. Syftet med genomlysningen var att säkerställa ett tillräckligt skydd för personuppgifter, oavsett om överföringen sker till tredje land. Det framgår av underlaget att en av de leverantörer som via sina underbiträden behandlar känsliga personuppgifter utanför EU/EES, mer specifikt i USA, var Visiba Group AB. Däremot nämns inte Microsoft i utredningen. Det framkommer av skriftlig återkoppling från regionen att Visiba efter genomlysningen kontaktades och att de inkom med en uppdaterad underbiträdeslista inklusive vidtagna säkerhetsåtgärder för överföring till tredjeland.

Vid sakgranskningen framkommer att Visiba Group AB:s underbiträden i tredjeland är kopplade till chattfunktionen, vilken är en tjänst som regionen inte använder. Enligt regionen förekommer därmed ingen tredjelandsöverföring.

<u>Intervjuer</u>
Det framgår av intervjuer att uppföljning av avtal sker på förekommen anledning och att det inte finns någon rutin eller annat systematiskt arbetssätt avseende uppföljning av avtal och leverantörer inom det granskade området. Det beskrivs att det funnits en ambition om att arbeta med uppföljning utifrån ett årshjul men att det varit svårt att hinna med detta och sedan 2022 har inte uppföljning genomförts.

Under tiden som tjänsterna används har ett fåtal incidenter upptäckts alternativt rapporterats av leverantör. Dessa har inte gett upphov till särskilda uppföljningar.

Vid intervjuer beskrivs även att uppdatering av underbiträden generellt sker genom att leverantörerna meddelar detta. Det sker i dagsläget inte någon proaktiv kontroll av underbiträden inom det granskade området.

Vidare beskrivs vidare att att leverantörer i övrigt följs upp genom kundgruppsmöten, strategiska möten med leverantören samt utvecklingsgrupperingar för specifika fall. Det har nyligen förts samtal avseende avtalsuppföljning med Platform24.

Bedömning
Har tjänsterna följts upp på ett ändamålsenligt sätt, avseende skydd av sekretessbelagda uppgifter och personuppgifter?

Delvis.

Några år tillbaka i tiden har vissa uppföljningar av leverantörer genomförts, vilket är positivt. Det är också positivt att alla de granskade avtalen avseende digitala vårdmöten innehåller villkor avseende uppföljning och att dessa i de flesta fall medger en relativt omfattande insyn. Det är också positivt att leverantörerna i tre av fyra avtal har en skyldighet att genomföra egenkontroll, dokumentera denna och redovisa denna till regionen.

Utifrån det perspektivet hade det varit önskvärt att den typen av dokumentation hade begärts in av regionen. Revision av leverantörer och uppföljning av avtalsefterlevnad kan vara både komplicerat och resurskrävande, vilket gör det ännu viktigare att genomföra de åtgärder som är relativt enkla att åstadkomma.

Att regelbundet ta del av utfallet av egenkontrollerna är dessutom en bra metod för att proaktivt kunna prioritera vilka leverantörer som bör bli föremål för en mer omfattande uppföljning. I det fall incidenter sker eller andra typer av avvikelser uppstår, kan dessutom kontinuerlig dokumentation vara värdefull för att exempelvis fördela ansvar.

Vi bedömer att det även generellt saknas ett systematiskt arbetssätt avseende uppföljning av leverantörer och avtal inom detta område.

Interna regler, rutiner och vägledning

Revisionsfråga 5: Finns interna regler, rutiner och vägledning som reglerar och stödjer användningen av digitala vårdmöten?

Utgångspunkter

Digitala vårdmöten har blivit en alltmer integrerad del av hälso- och sjukvården, och det är därför viktigt att det finns regler, rutiner och vägledning som reglerar och stödjer deras användning. Kunskap och förståelse för hur tjänsten ska hanteras och användas är också indirekt viktiga aspekter av säkerhetsperspektivet; brister det i handhavandet riskerar även det säkraste systemet att hanteras på ett osäkert sätt som i sin tur kan skapa säkerhetsrisker för informationen i systemet.

Enligt MSB:s föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster ska leverantören (i detta fall regionen) ha interna regler och arbetssätt som säkerställer att medarbetarna har kunskap om säker hantering av information. Detta ska säkerställas genom att medarbetarnas kompetens upprätthålls genom utbildning, informationsinsatser och övning, både regelbundet och utifrån identifierat behov.[19]

Det framgår även av MSB:s vägledning Säkerhetsåtgärder i informationssystem att organisationen behöver verifiera att det finns nödvändig dokumentation för att drift, förvaltning och användare ska kunna behandla information och informationssystem på ett säkert sätt.[20]

Iakttagelser

[19] 9 §.
[20] Vägledning: Säkerhetsåtgärder i informationssystem S.21-22.

Rutinen *Distanskontakt - tillämpningsanvisning* (februari 2022) riktar till sig vårdgivare som vill erbjuda vårdbesök eller behandling genom digitalt vårdbesök inom Region Halland. Rutinen beskriver vilka rutiner som ska följas avseende bland annat registrering, journalföring och medicinska riktlinjer. Rutinen *Digital kommunikation med patient* (november 2023) syftar till att klargöra hur digital kommunikation i text, bild och video ska ske med invånare och patienter inom hälso- och sjukvården samt vilken information som får tas emot, skickas och på vilket sätt.

Dokumentet *Rutin: Videokonferens och chatt* (september 2022) innehåller riktlinjer för hur patientuppgifter och annan sekretessbelagd information ska hanteras under video-, chatt- och talsamtal. Det framgår av rutinen att patientuppgifter och annan sekretessbelagd information (exklusive säkerhetskyddsklassificerad information) får utbytas över video- och talsamtal då distanstrafiken är krypterad. Vidare får patientuppgifter och annan sekretessbelagd information inte användas vid chattfunktionen då denna information sparas i chatthistoriken. Vidare framgår att presentationsläge under ett samtal får användas men att varken inspelnings- eller transkriberingsfunktion (omvandling av tal till text) får användas när det digitala mötet innehåller patientuppgifter eller annan sekretessbelagd information.

Rutin: Sekretess och samtycken (november 2021) syftar till att ge en översikt över sekretess och samtyckesregler inom Region Halland. Dokumentet beskriver de olika aspekterna av sekretess som gäller för patientinformation och hur dessa regler ska tillämpas i olika situationer. Det täcker även ansvarsfördelning, undantag från sekretessen, och hur samtycke från patienter ska hanteras.

<u>Skyddade personuppgifter</u>
Vidare har Region Halland en framtagen rutin som beskriver hur skyddade personuppgifter för patienter, anställda, besökare med flera ska hanteras så att uppgifterna förblir skyddade*, Rutin: Skyddade uppgifter* (juli 2022). Det framgår av rutinen att det är respektive IT-systems objektägare som ska se till att IT-systemet kan hantera skyddade personuppgifter. Det framgår av *Rutin: Digital kontakt med patient* (november 2023) att möjligheten att hantera personer med skyddade personuppgifter är olika i de olika systemen. Vidare hänvisas till rutinen för respektive system. Det framkommer i *Rutin: Platform24 – chatt och videobesök* att personer med skyddade personuppgifter inte ska hanteras i Platform24, även i de fall där patienter själva söker vård via plattformen. Inom ramen för granskningen har motsvarande rutindokument för de övriga systemen inte kunnat identifieras.

<u>Specifika rutindokument för systemen</u>
Visiba Care
På Region Hallands vårdgivarwebb finns information om systemet Visiba Care (“*Vårdgivare Halland: Visiba Care*”, inhämtad februari 2025), inklusive manualer, guider, filmer och hänvisning till tillämpningsanvisningar.

Platform24
På Region Hallands vårdgivarwebb finns information om systemet att tillgå (“Vårdgivare Halland: Platform24”, inhämtad februari 2025). På vårdgivarwebben finns information

länkat avseende bland annat hur besök ska bokas och genomföras, frågor och svar under införandet av plattformar, felanmälan och support samt länkar till rutiner och manualer för användningen. Dessutom finns dokument för utbildning, däribland användarutbildning och hänvisning till en demomiljö med testpersoner som användaren rekommenderas genomföra efter användarutbildningen.

Microsoft Teams
I dokumentet *Rutin: Videokonferens och chatt* beskrivs översiktligt förhållningssättet till Microsoft Teams.

HOPE Solution
Inom ramen för granskningen har specifika rutindokument avseende HOPE Solution inte kunnat lokaliseras.

Intervjuer
Det framkommer under intervjuer med representanter från informationssäkerhetsavdelningen att avdelningen inte är rutinmässigt involverade när rutiner arbetas fram för nya IT-system inom regionen, utan att avdelningen kopplas in för specifika frågeställningar.

Bedömning
Finns interna regler, rutiner och vägledning som reglerar och stödjer användningen av digitala vårdmöten?

Delvis.
Det finns övergripande generella rutiner som stöd för hur patientuppgifter och annan sekretessbelagd information får hanteras inom regionen vid digitala vårdmöten.Vi bedömer vidare att det i allt väsentligt finns välutvecklade, specifika och ändamålsenliga rutiner för Visiba Care och Platform24. Avseende Microsoft Teams finns endast översiktliga rutiner och avseende HOPE Solution har vi inte kunnat identifiera några rutiner.

Avseende hanteringen av skyddade personuppgifter finns även där välutvecklade, specifika och ändamålsenliga rutiner utifrån ett övergripande perspektiv. Dessa hänvisar i sin tur vidare till instruktioner för varje specifikt system, men där saknar både Visiba Care, Teams och HOPE Solution instruktioner för hur skyddade personuppgifter ska hanteras. Sådana systemspecifika rutiner finns endast för Platform24.

Information till patienter och anhöriga

Revisionsfråga 6: Ges patienter och anhöriga information om behandlingen av deras personuppgifter vid de digitala vårdmötena i enlighet med gällande lagstiftning?

Utgångspunkter
En av de grundläggande rättigheterna enligt GDPR är rätten till information, vilket innebär att individer, däribland patienter och anhöriga, har rätt att veta hur och varför deras personuppgifter behandlas. Personuppgiftsansvariga organisationer, exempelvis regioner, behöver se till att information ges till den registrerade (i detta fall främst vårdsökande, patienter, anhöriga och anställda) på ett lättillgängligt sätt, i skriftlig form

(analogt eller digitalt) och med ett klart och tydligt språk.[21] Lättillgängligt innebär exempelvis att informationen inte ska behöva letas upp eller sökas efter och ges på ett sätt som är anpassat för situationen.[22] Klart och tydligt språk innebär bland annat att språket ska vara så enkelt som möjligt och anpassat till målgruppen.[23]

Av artikel 13 och 14 i GDPR framgår vilka kategorier av information som måste ges till de registrerade om behandlingen av deras personuppgifter. Bland annat inkluderar detta vem som ansvarar för uppgifterna, syftet med behandlingen, den rättsliga grunden för behandlingen, och vem som har tillgång till uppgifterna. Om data överförs utanför EU, måste skyddsåtgärder anges. Organisationer ska också informera om hur länge uppgifterna sparas och om individens rättigheter, såsom att få tillgång till, rätta, radera uppgifter och att ta tillbaka eventuellt samtycke. Informationen ska vara tydlig och uppdateras vid förändringar.

GDPR specificerar inte formatet för hur information enligt artiklarna 13 och 14 ges till de registrerade, men det är de personuppgiftsansvarigas ansvar att vidta lämpliga åtgärder för att säkerställa insyn.[24] GDPR specificerar heller inte när eller hur organisationen ska informera registrerade om ändringar i den information som tidigare lämnats. Av riktlinjer om öppenhet enligt GDPR framgår att viktiga ändringar som alltid bör kommuniceras inkluderar förändringar i behandlingens syfte, den personuppgiftsansvariges identitet eller hur de registrerade kan utöva sina rättigheter.[25] Även om integritetspolicyn inte ändras avsevärt, är det ändå rekommenderat att ge de registrerade tydliga påminnelser om policyn och var den kan hittas.[26]

Iakttagelser

Granskad dokumentation
På Region Hallands webbplats finns information om hur regionen samlar in och hanterar personuppgifter, varför de gör det, och hur personer kan utöva sina rättigheter (“*Region Halland: Så behandlar vi personuppgifter”,* inhämtat februari 2025). Vidare framgår vem som är personuppgiftsansvarig inklusive kontaktuppgifter, vilka som personuppgifterna delas med, var personuppgifterna behandlas samt hur länge personuppgifterna sparas. Informationen riktar sig till bland annat vårdsökande och studerande. Vidare hänvisas till separata webbplatser för ytterligare beskrivning av hur Region Halland samlar in personuppgifter, för vilka ändamål som personuppgifter behandlas och med vilken rättslig grund, för olika områden. Hur personuppgifter behandlas i regionens vårdregister (exempelvis journalsystem) framgår av “*Region Halland: Dina personuppgifter i våra vårdregister”* (inhämtat februari 2025). Den generella texten använder formuleringen “Varje gång du besöker någon vårdenhet i Region Halland”. Det finns ingen hänvisning

[21] IMY, https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/de-registrerades-rattigheter/, 2025-03-01
[22] Riktlinjer om öppenhet och information till registrerade, s.8, 12.
[23] Ibid., s. 9-10.
[24] Ibid., s.14.
[25] Riktlinjer om öppenhet och information till registrerade, s.17.
[26] Riktlinjer om öppenhet enligt förordning (EU) 2016/679 (nedladdad 2025-02-26). S.18.

avseende behandling vid digitala vårdmöten.

Webbplatserna innehåller information om och uppgifter till de personuppgiftsansvariga samt uppgifter till dataskyddsombudet, de anger syftet med behandlingen och den rättsliga grunden för detta. Vidare framgår vem som har tillgång till uppgifterna. När det gäller överföring av data utanför EU/EES, framgår det att skyddsåtgärder vidtas för att säkerställa en adekvat skyddsnivå, såsom standardavtalsklausuler. Region Halland informerar också om hur länge personuppgifter sparas, vilket är så länge de är nödvändiga för ändamålet, med hänsyn till arkiv- och gallringsregler. Vidare beskrivs individens rättigheter, inklusive rätten att få tillgång till, rätta, eller radera sina personuppgifter, samt rätt till begränsning, dataportabilitet och invändning mot behandling. Webbplatserna innehåller även information om rätten att klaga och hänvisningar till vart detta görs.

Under granskningen har vi även tagit del av broschyrer och affischer som generellt beskriver varför personuppgifter registreras i regionens vårdregister när en person söker vård, och hur dessa personuppgifter behandlas. Enligt uppgift från regionen har dessa bland annat använts på vårdcentraler och sjukhus.

Vi har även tagit del av den standardformulering som regionen använder i brevkallelse och i system. Det framgår av uppgifter från regionen, att Region Halland har en regionalt beslutad formulering som ska finns i alla brevkallelser (inklusive för digitala vårdmöten) som skickas från journalsystemet VAS. Formuleringen innehåller en hänvisning till information om hanteringen av personuppgiftsbehandlingar på regionens hemsida, *Region Halland: Så behandlar vi personuppgifter,* samt telefonnummer till Dataskyddsenheten. Det framkommer dock av uppgifter från regionen att digitala kallelser från VAS idag inte innehåller den beslutade standardformuleringen.

Utöver kallelser har vi inom ramen för granskningen tagit del av hur det ser ut för en patient som ansluter till den digitala tjänsten Platform24. I systemet finns skrivning som hänvisar användaren till regionens webbplats, *Region Halland: Dina personuppgifter i våra vårdregister.* Informationen finns att tillgå i systemet för alla som loggar in. När en patient ansluter till ett digitalt vårdmöte med hjälp av Visiba Care fås ingen motsvarande dokumentation. Däremot får vi uppgift från regionen om att en sådan informationstext är framtagen och avsikten är att det framgent ska säkerställas att den eller motsvarande text ska användas vid användning av tjänsten. Avseende Microsoft Teams och HOPE Solution har vi inte kunnat bekräfta hur information om personuppgiftsbehandling sker vid användning av de tjänsterna.

Bedömning

Ges patienter och anhöriga information om behandlingen av deras personuppgifter vid de digitala vårdmötena i enlighet med gällande lagstiftning?

Delvis.

Webbplatserna *Region Halland: Så behandlar vi personuppgifter* och *Region Halland: Dina personuppgifter i våra vårdregister* uppfyller de grundläggande kraven enligt

GDPR. Webbplatserna uppdaterades i januari respektive februari 2025, vilket tyder på att de hålls uppdaterade. Texten vid webbplatserna är formulerade på ett relativt enkelt språk.

Däremot bedömer vi att, utifrån det material vi fått tillgång till och kunnat bekräfta, det saknas tillräcklig specifik och tydlig information avseende hur personuppgifter behandlas vid digitala vårdmöten. Formuleringen “Varje gång du besöker någon vårdenhet i Region Halland” får anses främst tolkas som ett fysiskt besök, vilket innebär att informationen på hemsidan helt utelämnar digitala vårdmöten. Vid anslutning till möte via Platform24 finns åtminstone en hänvisning till den generella texten på hemsidan, men i övrigt har vi inte kunnat identifiera att någon specifik information ges alls.

Vi bedömer det även som bristfälligt att informationen i Platform24 finns under rubriken ”Synpunkter” vid anslutning eftersom det inte kan anses som en självklar rubrik för att få information om personuppgiftsbehandling.

Sammantaget innebär detta att vi bedömer det som relativt svårt, om inte omöjligt, att på ett lättillgängligt sätt få information om hur ens personuppgifter behandlas vid digitala vårdmöten.

Samlad bedömning

Utifrån genomförd granskning är vår samlade bedömning att regionstyrelsen **inte helt** säkerställt att digitala vårdmöten sker på ett ändamålsenligt och lagenligt sätt.

Det är en betydande brist att regionen inte har genomfört riskanalyser, konsekvensbedömningar samt lämplighetsbedömningar enligt gällande lagstiftning och interna riktlinjer. Detta skapar en betydande risk både för informationssäkerheten och för att regionen inte uppfyller GDPR och OSL. Däremot är det positivt att analyser och bedömningar åtminstone påbörjats för Visiba Care, där förnyad användning och avtal aktualiserats under 2025.

Det är också positivt positivt att både tjänste- och PUB-avtal finns för alla tjänster. De är i stora delar ändamålsenliga men innehåller till viss del brister i form av ofullständiga instruktioner samt oklarheter avseende olika avtalsparter. Avtalen med leverantörer tillhandahåller villkor för uppföljning, men regionen saknar ett systematiskt arbetssätt för att kontrollera leverantörernas avtalsefterlevnad. Detta försvårar leverantörskontrollen, vilket innebär en ökad risk för säkerhetsbrister.

Registerförteckningen av personuppgiftsbehandlingar uppfyller kraven i GDPR på en övergripande nivå men det är otydligt hur pass uppdaterat registret är. När det gäller rutiner och annan vägledning för hur patientuppgifter och annan sekretessbelagd information får hanteras inom regionen vid digitala vårdmöten, bedömer vi att dessa till viss del är ändamålsenliga. Dock saknas i vissa fall specifika rutiner och i vissa fall saknas instruktioner helt. Vi bedömer att den informationen som ges avseende personuppgiftsbehandling på generell nivå inom regionen är väl anpassad, men däremot är det svårt för patienter och anhöriga att på ett lättillgängligt sätt få fullständig information om hanteringen av deras personuppgifter vid specifikt digitala vårdmöten.

Rekommendationer

Regionstyrelsen rekommenderas att:

- Säkerställa att riskanalyser, konsekvensbedömningar enligt GDPR och lämplighetsbedömningar enligt OSL snarast genomförs,
- Säkerställa att lämplighetsbedömningar dokumenteras på ett sätt som innebär att det är tydligt att bedömningar har skett innan utlämning (det vill säga innan en tjänst tagits i bruk), och att OSL därmed efterlevs,
- Säkerställa att de brister och oklarheter avseende främst tjänsteavtal och dess koppling till PUB-avtal åtgärdas vid liknande anskaffningar framgent,
- Säkerställa att uppföljning av leverantörer och avtal initieras snarast, samt att ett systematiskt arbetssätt avseende uppföljning inom området etableras,
- Säkerställa att ett systematiskt arbetssätt etableras (kan med fördel göras genom användning av utvecklad teknik), som innebär att registerförteckningarna regelbundet uppdateras och kvalitetssäkras,
- Säkerställa att ändamålsenliga rutiner finns även på systemspecifik nivå,
- Säkerställa att väl anpassad information om personuppgiftsbehandling sker på ett lättillgängligt sätt vid digitala vårdmöten.

Sammanfattande bedömningar utifrån revisionsfrågor

Revisionsfråga	Bedömning	
Har ändamålsenlig riskanalys, konsekvensbedömning och lämplighetsbedömning genomförts innan implementering?	**Nej** Granskningen visar att regionen inte har genomfört och dokumenterat varken riskanalys, konsekvens-bedömning eller lämplighets-bedömning, på ett fullständigt sätt för någon av de tjänster som är godkända att använda för digitala vårdmöten. Det är dock tydligt att diskussioner avseende frågeställningarna har förts.	
Finns ändamålsenligt tjänste- och personuppgiftsbiträdesavtal med leverantören av tjänsten?	**Delvis** Tjänste- och PUB-avtal finns för alla tjänster. De är i stora delar ändamålsenliga men innehåller till viss del brister i form av ofullständiga instruktioner samt oklarheter avseende olika avtalsparter	
Är de personuppgiftsbehandlingar som digitala vårdmöten innebär, korrekt införda i regionstyrelsens register-förteckning över personuppgifts-behandlingar?	**Delvis** Registerförteckningen uppfyller på en övergripande nivå kraven i GDPR och de system som används för digitala vårdmöten är inkluderade i registret. Däremot är registret inte komplett ifyllt för alla system. Det är dessutom inte tydligt hur uppdaterat registret är avseende de fyra systemen.	
Har tjänsten följts upp på ett ändamålsenligt sätt, avseende skydd av sekretessbelagda uppgifter och personuppgifter?	**Delvis** Regionen har tidigare genomfört vissa uppföljningar av leverantörer. De granskade avtalen innehåller villkor för uppföljning och det är positivt att leverantörerna i majoriteten av avtalen är skyldiga att genomföra och dokumentera egenkontroller samt rapportera	

	dessa till regionen. Dock skulle det vara önskvärt att regionen aktivt begär in denna dokumentation. Granskningen visar att det generellt saknas ett systematiskt arbetssätt för uppföljning av leverantörer och avtal inom detta område.	
Finns interna regler, rutiner och vägledning som reglerar och stödjer användningen av digitala vårdmöten?	**Delvis** Det finns generella rutiner för hantering av patientuppgifter annan sekretessbelagd information vid digitala vårdmöten. Det varierar hur välutvecklade och ändamålsenliga de specifika rutinerna är för de olika systemen, och ett system saknar identifierade rutiner. När det gäller hanteringen av skyddade personuppgifter finns det övergripande välutvecklade rutiner, men specifika instruktioner saknas för tre av de fyra systemen.	
Ges patienter och anhöriga information om behandlingen av deras personuppgifter vid de digitala vårdmötena i enlighet med gällande lagstiftning?	**Delvis** Webbplatserna med information om person-uppgiftshanteringen uppfyller de grundläggande kraven enligt GDPR. Däremot bedömer vi att det saknas specifik och tydlig information avseende hur personuppgifter behandlas vid digitala vårdmöten. Vi bedömer det som relativt svårt, om inte omöjligt, att på ett lättillgängligt sätt få information om hur ens personuppgifter behandlas vid digitala vårdmöten.	

2025-04-08

Marie Lindblad	Charlotte Arnell
Uppdragsledare	*Projektledare*

Denna rapport har upprättats av Öhrlings PricewaterhouseCoopers AB (org nr 556029-6740) (PwC) på uppdrag av Region Halland enligt de villkor och under de förutsättningar som framgår av projektplan från den 12 mars 2024. PwC ansvarar inte utan särskilt åtagande, gentemot annan som tar del av och förlitar sig på hela eller delar av denna rapport.

Bilaga - Förteckning av granskad dokumentation

Riskanalyser, konsekvensbedömningar och lämplighetsbedömningar

- Visiba
  - Konsekvensbedömning avseende dataskydd för Visiba (februari 2025)
- Microsoft Teams
  - Riskanalyser - Projekt övergång till Microsoft 365 (odaterad)
  - Delrapport riskanalyser - Projekt Övergång till Microsoft 365 (maj 2021)
- Platform24
  - Konsekvensbedömning avseende dataskydd för Platform24 (utkast från oktober 2022 och utkast från oktober 2023)
- Hope
  - Konsekvensbedömning avseende dataskydd för HOPE Solution (juni 2019)

Tjänsteavtal

- Visiba:
  - Avtal Visiba (undertecknad november 2017)
  - Leveransavtal avseende Visiba Care (februari 2025) inklusive offert (januari 2024)
- Microsoft Teams:
  - Villkor för onlinetjänster (januari 2016)
  - Villkor för onlinetjänster (september 2017)
  - Dataskyddstillägg för Microsofts professionella tjänster (september 2022)
  - Microsofts molntjänster & svenska krav på integritet och patientdatasäkerhet (2017)
- Avtal Platform24 (version 1.2, RS210939, undertecknad september 2021)
- Avtal: Prenumerationsvillkor för HOPE Solution (undertecknad juni 2019)

Personuppgiftsbiträdesavtal

- Visiba Care:
  - Personuppgiftsbiträdesavtal mellan personuppgiftsansvarig och personuppgiftsbiträde avseende Visiba Care (undertecknad mars-maj 2018)
  - Personuppgiftsbiträdesavtal mellan den personuppgiftsansvarige och
  - personuppgiftsbiträdet avseende tillhandahållandet av digitala vårdmöten (februari 2025)
  - Instruktioner vid behandling av personuppgifter för Region Halland Visiba Care (odaterad)
  - Personuppgiftspolicy (april 2018)
  - Bilaga B: Lista över underbiträden (undertecknad april 2021)

- Personuppgiftsbiträdesavtal Platform24 Healthcare AB (undertecknad oktober 2021)
- Personuppgiftsbiträdesavtal Addi Medical AB (HOPE Solution) (undertecknad december 2022)

Registerförteckningar över personuppgiftsbehandlingar

- Utdrag registerförteckning Visiba Care (skärmdump, januari 2025)
- Registerförteckningen Microsoft Teams (odaterad)
- Registerförteckningen Platform24 (odaterad)
- Registerförteckning HOPE Solution (skärmdump, odaterad)

Uppföljning

- Revision av tekniska och organisatoriska säkerhetsåtgärder och åtaganden gentemot underbiträden i enlighet med personuppgiftsbiträdesavtalet, Visiba Group, inklusive personuppgiftsbiträdesavtal Glesys och Twilio-Sengrid, (augusti 2019)
- Presentationsmaterial: Utredning gällande överföring av personuppgifter till tredje land (april 2021)

Interna regler, rutiner och vägledning

- Rutin: Videokonferens och chatt (september 2022)
- Rutin: Vårdkontakter - registrering (februari 2024)
- Rutin: Platform24 - chatt och videobesök (februari 2024)
- Rutin: Medicinsk service för distanskontakt (februari 2024)
- Rutin: Journaldokumentation (juli 2024)
- Rutin: Distanskontakt - tillämpningsanvisning (februari 2022)
- Rutin: Digital kommunikation med patient (november 2023)
- Rutin: Skyddade personuppgifter (juli 2022)
- Rutin: Sekretess och samtycken i vården (november 2011)
- Region Hallands vårdgivarwebb

Information för patienter och anhöriga avseende behandling av deras personuppgifter

- Region Halland: Så behandlar vi dina personuppgifter (inhämtat februari 2025), https://www.regionhalland.se/dataskydd
- Region Halland: Dina personuppgifter i våra vårdregister, (inhämtat februari 2025), https://www.regionhalland.se/om-region-halland/sa-behandlar-vi-personuppgifter/dina-personuppgifter-i-vara-vardregister
- Broschyr: Dina personuppgifter i våra vårdregister (2018)
- Affisch: Dina personuppgifter i våra vårdregister (odaterad)

Riktlinjer, rutiner och övrigt

- Riktlinje: 309 Informationssäkerhet RH (december 2022)
- Riktlinje: Riktlinje för inköp och upphandling (januari 2024)

- Rutin: Personuppgiftsbiträdesavtal (PUB-avtal) i upphandlingar (oktober 2020)
- Rutin: Konsekvensbedömning avseende dataskydd (DPIA) (januari 2022)
- Säkerhet - Riktlinjer för Informationssäkerhet och dataskydd (2018)