Granskning av hantering av personuppgifter och sekretess vid digitala vårdmöten

Region Örebro läns revisorer

Mars 2026

Sammanfattning

PwC har på uppdrag av revisorerna i Region Örebro län genomfört en granskning av hantering av personuppgifter och sekretess vid digitala vårdmöten. Granskningens syfte var att bedöma om hälso- och sjukvårdsnämnden och regionstyrelsen har säkerställt att digitala vårdmöten sker på ett ändamålsenligt och lagenligt sätt.

Utifrån genomförd granskning är vår samlade bedömning att Region Örebro län *inte helt* säkerställt att digitala vårdmöten bedrivs på ett ändamålsenligt, lagenligt och informationssäkert sätt. De identifierade bristerna återfinns inom samtliga sex granskningsområden och visar att hälso- och sjukvårdsnämnden behöver utveckla sin riskhantering inom området, säkerställa ändamålsenliga och uppdaterade avtal samt allmänt sammanhållet, systematiskt och dokumenterat arbetssätt för att uppfylla krav enligt GDPR, offentlighets- och sekretesslagen samt god intern kontroll. Sammantaget medför detta en förhöjd risk för bristande regelefterlevnad och ett otillräckligt skydd av sekretessbelagda uppgifter och känsliga personuppgifter.

Den mest betydande svagheten rör avsaknad av genomförda och uppdaterade riskanalyser, konsekvensbedömningar enligt GDPR och lämplighetsbedömningar enligt OSL, såväl inför som under användning av tjänsterna. I kombination med en bristfällig avtalsstruktur blir ansvar, roller och skyddsnivåer oklara i praktiken. Tjänsterna följs inte heller upp på ett systematiskt eller dokumenterat sätt, vilket ytterligare försvagar nämndens kontroll över hantering av sekretessbelagda uppgifter och personuppgifter.

De aktuella personuppgiftsbehandlingar är inte korrekt införda i den registerförteckning som krävs enligt artikel 30 GDPR. Därtill förs behandlingsregistret genom manuell hantering i fysiska pärmar, vilket medför risk för bristande transparens och svårigheter att visa en aktuell registerförteckning vid tillsyn.

Avseende instruktioner för användning av tjänsterna och allmän utbildning kring informationssäkerhet/digital informationshantering finns viss styrning på plats, men inte i sådan omfattning eller detaljnivå att de reglerar och stödjer användningen av digitala vårdmöten.

Granskningen visar även att det inte kan säkerställas att patienter och anhöriga får fullständig och lagenlig information om hur deras personuppgifter behandlas vid digitala vårdmöten.

Sammanfattningsvis behöver hälso- och sjukvårdsnämnden förstärka arbetet inom alla sex granskningsområden för att säkerställa en säker, strukturerad och lagenlig hantering av digitala vårdmöten. Nämnden uppger att förbättringsarbete pågår, bland annat införande av informationsklassning och riskanalys, med tillhörande årshjul för uppföljning. Detta förändrar dock inte bedömningen, då bristerna är omfattande och innebär betydande risker för otillräckligt skydd av personuppgifter, bristande spårbarhet och otillräcklig regelefterlevnad.

Nedan ses bedömning för varje revisionsfråga. För fullständiga bedömningar se respektive revisionsfråga i rapporten eller det avslutande avsnittet “Sammanfattande bedömningar utifrån revisionsfrågor”.

Revisionsfrågor	Bedömning	
Har ändamålsenlig riskanalys, konsekvensbedömning och lämplighetsbedömning genomförts innan implementering?	Nej	
Finns ändamålsenligt tjänste- och personuppgiftsbiträdesavtal med leverantör av tjänsten?	Delvis	
Är de personuppgiftsbehandlingar som digitala vårdmöten innebär, korrekt införda i regionstyrelsens registerförtäckning över personuppgiftsbehandlingar?	Nej	
Har tjänsten följts upp på ett ändamålsenligt sätt, avseende skydd av sekretessbelagda uppgifter och personuppgifter?	Nej	
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

Hälso- och sjukvårdsnämnden rekommenderas att:

1. Genomföra ändamålsenliga risk-, konsekvens- och lämplighetsbedömningar för de digitala vårdtjänster där detta är tillämpligt

Nämnden behöver genomföra och dokumentera fullständiga riskanalyser, konsekvensbedömningar enligt GDPR och lämplighetsbedömningar enligt OSL för de digitala tjänster där lagstiftningen kräver det. Eftersom bristerna i dagsläget är så stora behöver dessa analyser och bedömningar genomföras omgående.

2. Säkerställa korrekta, fullständiga och uppdaterade avtal.

Nämnden behöver säkerställa att samtliga relevanta tjänste- och personuppgiftsbiträdesavtal är fullständiga, korrekta och återkommande följs upp tillsammans med respektive leverantör. Avtalen behöver även vara lämpliga i relation till vilka uppgifter som behandlas i de aktuella tjänsterna, vilket tydliggörs i samband med rekommendationen i punkt 1.

3. Införa ett digitalt och systematiskt behandlingsregister

Dagens manuella hantering bör ersättas med ett digitalt, strukturerat och kontinuerligt uppdaterat register enligt artikel 30 GDPR, där alla aktuella personuppgiftsbehandlingar dokumenteras och hålls uppdaterade.

4. Följa upp att leverantörerna efterlever avtalade krav

Nämnden bör genomföra regelbunden och dokumenterad uppföljning av att leverantörer uppfyller de krav och åtaganden som avtalats. Ett första steg är att genomföra den uppföljning som redan idag är möjlig i de befintliga avtalen, endast genom begäran av olika typer av dokumentation.

5. Stärka rutiner och utbildning kring användning och digital informationshantering

Rutiner och instruktioner för användningen av de digitala verktygen bör tydliggöras. Även utbildning kring informationssäkerhet och digital informationshantering bör stärkas. Kombinerat med detta behöver det säkerställas att kunskapsnivåerna inom området ges till nya medarbetare samt upprätthålls över tid.

6. Säkerställa fullständig och lagenlig informationsgivning till patienter och anhöriga

Det behöver säkerställas att informationsgivningen enligt GDPR är både korrekt och fullständig, exempelvis genom att utveckla informationen som finns på regionens hemsida.

Innehållsförteckning

Förkortningar och begrepp

CSL	Cybersäkerhetslag (2025:1506).
EDPB	Europeiska dataskyddsstyrelsen är ett oberoende organ som har till uppgift att se till att den allmänna dataskyddsförordningen (GDPR) och dataskyddsdirektivet tillämpas på samma sätt i EU-länderna och i Norge, Liechtenstein och Island.
Gateway	En teknisk komponent som fungerar som en brygga mellan två olika system, så att de kan kommunicera med varandra trots att de använder olika tekniska standarder.
GDPR	Den allmänna dataskyddsförordningen EU (2016/679).
IMY	Integritetsskyddsmyndigheten.
Informationssäkerhet	Det finns ingen legal eller formellt fastslagen definition av informationssäkerhet. 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.
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.
Känslig personuppgift	Uppgift som bedöms särskilt skyddsvärd, i enlighet med art. 9 GDPR. Exempel på känsliga personuppgifter är uppgifter om hälsa, sexuell läggning, etnicitet eller politisk åsikt.
MCF	Myndigheten för civilt försvar (tidigare MSB: Myndigheten för samhällsskydd och beredskap).
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.
NIS2	Network and Information Systems Directive 2. Syftar till att öka cybersäkerhetsnivån inom EU och därigenom öka motståndskraften och förbättra förutsättningarna för EU:s inre marknad.

On-prem lösning	Betyder att ett IT-system finns och sköts i organisationens egna lokaler, på deras egna servrar, i stället för att ligga hos en extern leverantör på internet. Organisationen ansvarar själv för drift, uppdateringar och säkerhet.
OSL	Offentlighets- och sekretesslag (2009:400).
PDL	Patientdatalag (2008:355).
Personuppgiftsbehandling/behandlingar	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 Örebro Län 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.
SKR	Sveriges Kommuner och Regioner.
Skyddade personuppgifter	Den som är utsatt, eller riskerar att utsättas, för brott kan i vissa fall få skyddade personuppgifter. Det finns tre typer av skyddade personuppgifter: sekretessmarkering, skyddad folkbokföring och fingerade personuppgifter. Det är Skatteverket som fattar beslut om sekretessmarkering och skyddad folkbokföring.
Underbiträde	Underbiträde är den som behandlar personuppgifter för personuppgiftsbiträdets 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.

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 GDPR 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. Om personuppgifter hanteras dåligt kan det minska förtroendet för regionen, offentlig sektor och välfärdssystemet. 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.

Regionens revisorer har mot bakgrund av ovanstående, samt genomförd väsentlighets- och riskbedömning, beslutat att granska hanteringen av personuppgifter och sekretessbelagda uppgifter vid digitala vårdmöten. Granskningen ingår i revisionsplanen 2025.

Syfte och revisionsfrågor

Syftet med granskningen har varit att bedöma om hälso- och sjukvårdsnämnden och regionstyrelsen har säkerställt att digitala vårdmöten sker på ett ändamålsenligt och lagenligt sätt.

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)
- Cybersäkerhetslag (2025:1506)
- 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
- Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården, HSLF-FS 2016:40

Avgränsning

Granskningsobjekt är hälso- och sjukvårdsnämnden (HSN) och granskningen har i huvudsak omfattat år 2025. Granskningen har avsett möten med patient som sker över video. Granskningen har avgränsats till de system/tjänster som används i regionens egen verksamhet (det vill säga privata vårdgivare omfattas inte av granskningen).

Metod

Granskningen har genomförts genom intervjuer och dokumentstudier. Insamling har skett av framförallt dokumenterade riskanalyser och bedömningar, avtal, dokumenterade uppföljningar, interna styrande och stödjande dokument och information avseende digitala vårdmöten som ges till patienter och anhöriga. Digitala intervjuer har hållits med tjänstepersoner med ansvar för styrning, drift och uppföljning av digitala vårdmöten.

Intervjuade funktioner:

- Enhetschef Digitala Vårdmiljöer
- Verksamhetsutvecklare/Projektledare Digitala Vårdmiljöer
- Objektledare IT
- Region Service IT
- Projektledare E-hälsa och Digitalisering
- Verksamhetsspecialister

De intervjuade har beretts möjlighet att sakgranska rapporten. Rapporten har kvalitetssäkrats i enlighet med PwC:s interna rutiner och checklistor för kvalitetssäkring.

Granskningsresultat

Organisation
Hälso- och sjukvårdsnämnden (HSN) i Region Örebro län ansvarar för att tillgodose invånarnas behov av hälso- och sjukvård och är i huvudsak personuppgiftsansvariga för den personuppgiftsbehandling som sker inom ramen för nämndens verksamhet.[1]. Nämnden har ett uppdrag att erbjuda användarvänliga digitala lösningar till länets invånare, organisationer och företag i linje med kravet om ”Digitalt först”. De digitala lösningarna ska vara effektiva, tidsbesparande, kvalitetssäkrade och säkra ur integritetsperspektiv. [2]

Den operativa genomförandeförmågan för digitalisering i vården är organiserad inom enheten Digitala Vårdmiljöer, placerad i hälso- och sjukvårdsförvaltningen, enligt uppgift vid intervju. Enheten arbetar med digitalisering av vårdverksamheten, inklusive stöd kring journalsystem och digitala vårdtjänster. Digitala Vårdmiljöer uppgavs vara relativt ny (cirka fyra–fem år) och består av omkring ett tjugotal medarbetare, främst verksamhetsutvecklare, objektägare och objektledare. Innan enheten etablerades låg motsvarande uppdrag inom regionens IT-funktion. Enheten samverkar nära jurist- och informationssäkerhetsfunktionerna, bland annat i frågor om informationsklassning.

Sammantaget beskrivs att HSN beslutar om inriktning och krav, inklusive digitaliseringsmålen, medan Digitala Vårdmiljöer ansvarar för det operativa genomförandet och samverkar med stödjande funktioner (juridik och informationssäkerhet) för att säkerställa rättslig efterlevnad och god informationssäkerhet i den digitala vårdmiljön.

Inom Region Örebro län genomförs digitala vårdmöten med stöd av flertal digitala verktyg. Av både intervjuer och stödjande dokumentation framgår att regionen använder flera olika plattformar för såväl patientmöten som vårdinternt samarbete. De system som används för digitala vårdmöten är Pexip, Visiba Care, och Platform24. Visiba Care används för digitala möten med patienter. Platform24 fungerar som digital ingång och triagetjänst via 1177 Direkt.

Nedan följer en beskrivning av system som används för digitala vårdmöten i Region Örebro län.

Digitala vårdmöten i Pexip
Pexip är Region Örebro läns lokalt installerade videokonferenssystem och driftas i regionens egna serverhallar. Systemet används främst för interna vårdmöten, såsom multidisciplinära konferenser (MDK). Patienter deltar normalt inte i Pexip-möten, men det kan förekomma i undantagsfall. Dock diskuteras patienter och dess uppgifter under mötena, och därför behandlas känsliga personuppgifter och sekretessbelagd information i verktyget. Ingen extern part har åtkomst till systemets bakomliggande funktioner, och enligt intervjuer tar leverantören endast emot loggar utan personuppgifter. Pexip kan även fungera som brygga till Microsoft Teams, vilket möjliggör deltagande i Teamsmöten via Pexip-ansluten utrustning.

[1] Bestämmelser för politiska organ inom Region Örebro, gällande från 1 januari 2023, datum samt dnr saknas.
[2] Verksamhetsberättelse: Hälso- och sjukvårdsnämnden, helår 2025, https://www.regionorebrolan.se/contentassets/bd02d9468c0f4cbe92e689165fa5feb5/verksamhetsberattelse-2025---halso--och-sjukvardsnamnd.pdf, 2026-03-12.

Digitala vårdmöten i Visiba Care
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. Systemet levereras som en tjänst och inkluderar licens för programvara, underhåll och support. Tjänsten är molnbaserad, vilket innebär att den levereras över internet. Visiba Care används för digitala möten med patienter och möjliggör både videobesök och annan digital kommunikation inom vården. Visiba Care hanterar skyddsvärda personuppgifter i samband med digitala vårdmöten och fungerar som den primära digitala mottagningen för patientkontakter.

Digitala vårdmöten i Platform24
Platform24 är en molnbaserad tjänst som regionen köper via Inera och används som digital ingång för invånare via 1177 Direkt. Tjänsten stödjer automatiserat triage, chatt, digital bedömning och självhjälpsfunktioner, och utgör därmed en central del av regionens digitala patientflöden. Region Örebro Län använder samtliga funktioner i Platform24; video, chatt och triagering.

Risk-, konsekvens- och lämplighetsbedömning

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

Utgångspunkter
Riskanalyser
Riskanalyser avseende informationssäkerhet (som är en nödvändig förmåga för att skydda bland annat personuppgifter och sekretesskyddade uppgifter) 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 cybersäkerhetslagen[3] och Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården.[4] Innan cybersäkerhetslagen trädde i kraft var det också obligatoriskt enligt MSB:s föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster (MSBFS 2018:8).

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 säkerhetsåtgärder som behöver vidtas för att uppnå ett adekvat skydd. Om riskanalyser inte genomförs på ett ändamålsenligt sätt, och kontinuerligt hålls uppdaterade, 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

[3] 2 kap. 3 § p. 1, 4, 5.
[4] 3 kap. 5 §

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 GDPR[5] 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 vägledning som är framtagen av Integritetsskyddsmyndigheten (IMY).[6] 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 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 Örebro Län 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 myndighet har det yttersta ansvaret för att säkerställa att informationen hanteras på ett ändamålsenligt sätt och i enlighet med gällande lagar. Enligt OSL[7] 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 däremot förarbetena[8] till lagregeln 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

[5] Art. 35.1
[6] https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/konsekvensbedomning/nar-ska-en-konsekvensbedomning-genomforas/, 2026-03-12.
[7] 10 kap. 2 a §.
[8] Proposition 2022/23:97, s. 17.

karaktär. Vidare framgår av eSams vägledning *Utkontraktering – sekretess och dataskydd*[9] att det är viktigt att den utkontrakterande myndigheten noggrant dokumenterar den utredning och bedömning som myndigheten genomför inför utkontraktering. 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.

Iakttagelser

Pexip

Dokumentation

Granskning av erhållen dokumentationen, *Informationssäkerhetsanalys-med-klassning (Pexip)*, har genomförts. Informationssäkerhetsanalysen daterad 2021 innehåller en riskanalys med nio identifierade risker samt beskrivningar av orsaker och föreslagna åtgärder. Flera delar saknar dock centrala komponenter, såsom angiven metod för uppföljning, tidpunkt för uppföljning, beslut och ansvarig funktion. Av analysen framgår också att systemskisser med säkerhetsanalyser, beroenden och driftdokumentation saknas. Vidare visar den granskade dokumentationen att loggar i Pexip innehåller personuppgifter, exempelvis e-postadresser och IP-adresser. vilket tyder på att personuppgifter och möjligtvis sekretessbelagda uppgifter kan lämnas ut till leverantör. Någon konsekvensbedömning enligt GDPR eller lämplighetsbedömning enligt OSL har inte genomförts.

Intervju

Vid intervjuer beskrivs att det genomfördes en informationssäkerhetsanalys inför införandet av Pexip under 2021. Analysen har inte uppdaterats sedan dess, och någon ny riskanalys eller strukturerad uppföljning har inte genomförts. Enligt intervjuer har viss intern uppföljning förekommit, men denna har inte dokumenterats. Det beskrivs även att nämnden avser att revidera den befintliga informationsklassningen i samband med införandet av arbetssätt enligt KLASSA.[10] Det bekräftas att konsekvensbedömning enligt GDPR eller lämplighetsbedömning enligt OSL inte har genomförts.

Vid intervjuer förklaras också att Pexip är lokalt installerad och att inga uppgifter lämnas ut till leverantören. Vid support och felsökning kan loggar från systemet lämnas till leverantör, men dessa innehåller enligt nämnden inga person- eller sekretessbelagda uppgifter.

Visiba Care

Dokumentation

PwC har tagit del av en informationssäkerhetsanalys genomförd 2019 avseende Visiba Care version 1.2. Analysen innehåller systembeskrivning och klassning, härledda säkerhetskrav, identifierade risker samt övergripande hänvisningar till PDL- och GDPR-aspekter med föreslagna åtgärder.

I underlaget saknas konsekvent och motiverad bedömning av sannolikhet och konsekvens per risk. Spårbarheten från identifierade risker till konkreta kontroller eller krav, ansvar och tidsplan är svag, och

[9] Dnr ES2023-06, s. 32–33.

[10] Den metodik med tillhörande it-stöd som SKR tillhandahåller.

under flik 3.3 Sammanfattning analys saknar flera krav sammanfattade åtgärdsförslag och utsedd ansvarig. Underlaget innehåller uppgifter om brister kopplade till behörighetskrav för informationstillgångar. Formellt godkännande inför drift har inte redovisats i materialet.

I analysen uppges att Visiba Care inte hanterar skyddade personuppgifter. I det styrande dokumentet Ansvar och säkerhet vid digitala möten[11] anges att digitala vårdmöten mellan patient och vårdpersonal innebär behandling av känsliga personuppgifter och sekretessbelagd information och att Visiba Care ska användas för sådana möten. PwC har inte tagit del av någon uppdaterad riskanalys eller kompletterande bedömning som visar revidering eller förstärkning efter 2019.

Någon konsekvensbedömning enligt GDPR eller lämplighetsbedömning enligt OSL har inte genomförts.

Intervjuer

Vid intervjuer uppges att nämnden genomförde en riskanalys för Visiba Care i form av en informationssäkerhetsanalys år 2019. Vid intervjuer uppgavs att avvikelserna i informationssäkerhetsanalysen från 2019 arbetades vidare med, dock dokumenterades inte detta uppföljningsarbete. De intervjuade uppger att arbetet troligen fördes vidare i dialog med leverantören, men det finns inga dokumenterade underlag som bekräftar detta. Riskanalysen har, så vitt de intervjuade känner till, internt inte följts upp eller uppdaterats sedan 2019.

Vid intervjuerna bekräftas att ingen konsekvensbedömning enligt GDPR eller lämplighetsbedömning enligt OSL har genomförts. Man uppger vid intervjuer att vid införandet av Visiba Care så var kunskapen om GDPR och relaterade begrepp begränsad varav ingen formell konsekvensbedömningen skedde. De intervjuade understryker vidare att ingen journalföring eller dokumentation sker i Visiba Care.

Vid intervju diskuteras att det i riskanalysen uppges att det i Visiba Care inte hanteras skyddade personuppgifter, medan det i en arbetsrutin beskrivs att Visiba Care ska användas för sekretessbelagd information (skyddade personuppgifter är en typ av sekretessbelagd information). De motsägelsefulla uppgifterna förklaras vid intervjun med att det initialt var planerat att Visiba Care ej skulle hantera skyddade personuppgifter men att detta beslut reviderades. Dock finns inte det reviderade beslutet, inklusive motivering eller analys, dokumenterad. Det har inte heller genomförts uppdateringar eller kompletteringar av riskanalysen med anledning av detta.

Platform24

Dokumentation

Platform24 är en tjänst som Region Örebro län köper in via Inera, och det underlag som delats i granskningen utgörs delvis av dokumentation framtagen av Inera. I det material som nämnden tillhandahållit finns ingen riskanalys som specifikt avser Platform24 genomförd av nämnden.

Det dokumenterade underlaget består främst av *Kopia av 1177 direkt - RÖL:s informationssäkerhetsanalys-med-klassning* utförd 2023. Analysen avser den bredare tjänsten 1177 Direkt och inte specifikt de digitala vårdmötena. Riskanalys beskriver flertal risker, ett antal förslag på åtgärder men ingen dokumenterad uppföljning av åtgärder. Inga risker kopplat till digitala vårdmöten

[11] Ansvar och säkerhet vid digitala möten, dnr 15RS2466, giltigt från 2022-04-11.

finns upptagna i analysen. Ett flertal säkerhetskrav är angivet under fliken “Säkerhetsåtgärder” i informationssäkerhetsanalysen. Det är inte dokumenterat huruvida säkerhetskraven uppfylls eller ej. I analysen uppges även vilka som deltagit i genomförandet av analysen och funktioner kopplat till informationssäkerhet. Av deltagarförteckningen framgår att kompetens kopplat till juridik, dataskydd och eventuellt även informationssäkerhet har saknats vid genomförandet av riskanalysen. Det framstår inte heller som om analysen är färdigställd eftersom många fält är tomma (flertalet risker är exempelvis inte värderade) och de upptagna riskerna är relativt få för den här typen av analyser (19).

Vi har även tagit del av dokumentet *Dataskyddskonsekvensbedömning Inera*. Namnet till trots är detta ingen konsekvensbedömning, utan endast en kortare bedömning för att besvara frågan om en konsekvensbedömning enligt GDPR behöver göras eller ej. Den är genomförd utifrån Ineras roll som personuppgiftsbiträde och avser endast tjänsterna symptombedömning och hänvisning. Inera bedömer själva i dokumentet att de behöver göra en konsekvensbedömning.

I dokumentet framgår även explicit att varje kund i sin roll som personuppgiftsansvarig måste göra en egen konsekvensbedömning för att säkerställa regelefterlevnad och adekvat säkerhetsnivå. En sådan har inte lämnat till PwC inom ramen för denna granskning. Nämnden har överlämnat dokumentet *Konsekvensbedömning 1177 direkt*. Dokumentet är en kortfattad och inte fullständig konsekvensbedömning som Region Uppsala genomfört för tjänsterna symptombedömning och hänvisning inom ramen för 1177 Direkt.

Inom ramen för denna granskning har vi inte emottagit någon lämplighetsbedömning enligt OSL avseende Platform24.

Intervjuer

Vid intervjuer bekräftas att nämnden inte har genomfört vare sig riskanalys, konsekvensbedömning enligt GDPR eller lämplighetsbedömning enligt OSL. Intervjuade beskriver att nämnden i stor utsträckning har förlitat sig på material som Inera tagit fram. Vid intervjuerna framkommer även att man saknar rutiner för att säkerställa att risk- och konsekvensbedömningar alltid genomförs vid införande av nya digitala vårdtjänster. Intervjupersonerna uppger att arbetet i dag är personberoende och att varken informationssäkerhetsfunktionen eller dataskyddsorganisationen systematiskt involveras.

Vidare beskrivs att arbetet är under förändring och att framgent avses en bättre systematik vara etablerad. Det planeras bland annat för att KLASSA systematiskt ska användas samt att ett årshjul ska införas för att bland annat uppföljning och uppdatering ska säkerställas.

Bedömning

Har ändamålsenlig riskanalys, konsekvensbedömning och lämplighetsbedömning genomförts innan implementering?

Nej

Granskningen visar att hälso- och sjukvårdsnämnden inte har genomfört, genomfört på ett fullständigt sätt eller dokumenterat varken riskanalys, konsekvensbedömning eller lämplighetsbedömning för någon av de tjänster som är godkända att använda för digitala vårdmöten.

Samtliga riskanalyser, i de fall de är påbörjade, är ofullständiga, saknar tydliga ägare av risker och åtgärder, och ingen uppföljning eller aktualisering av befintliga analyser har genomförts. Sammantaget innebär det att vi bedömer att hälso- och sjukvårdsnämnden saknar ett systematiskt arbetssätt inom detta område.

Avseende Pexip finns uppenbarligen även en oklarhet i vilken utsträckning leverantören har tillgång till personuppgifter eller ej. Situationen riskerar att leda till att sekretessbelagd information oavsiktligen och oreglerat delas med leverantör, vilket utgör en allvarlig risk. Det är också den typen av oklarheter som kan undvikas om en fullständig riskanalys och konsekvensbedömning görs, eftersom dessa processer inkluderar analyser av flödena av uppgifter mellan kund och leverantör.

Vi bedömer även, både utifrån tillhandahållet material och intervjuer, att medvetenhet och kunskap kring regelverk inom området brister.

Sammantaget innebär detta en stor risk för att nämnden inte följer gällande lagstiftning inom området. Det går heller inte att utesluta, utifrån nämndens bristande kontroll, analys och uppföljning, att patienters och anhörigas person- och sekretessbelagda uppgifter inte skyddas på ett adekvat sätt.

Leverantörsavtal: ändamålsenligt 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).

Exempel på villkor som bör finnas med är krav på säkerställande av sekretesskyddad information (som inte alltid är personuppgifter), krav på olika typer av säkerhetsåtgärder (både tekniska och organisatoriska), effektiva sanktioner och medel i det fall leverantören inte lever upp till ställda krav, samt möjliggörande av effektiv insyn och uppföljning.

När det gäller PuB-avtalet är det obligatoriskt enligt GDPR när personuppgifter ska behandlas på uppdrag av en personuppgiftsansvarig (PuA). PuA behöver, både genom kravställning i upphandlingen och genom villkor i 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 ska kunna behålla kontrollen över personuppgiftsbehandlingen.

Iakttagelser

Pexip

Utifrån uppgiften att Pexip är lokalt installerad, vilket innebär att inga uppgifter eller information överförs eller tillgängliggörs till leverantören, har avtal för detta system inte granskats.

Visiba Care

Dokumentation, tjänsteavtal
PwC har tagit del av *Leveransavtal Avseende Visiba Care*, daterat 18 juni 2025. Avtalet är tecknat med Atea i deras roll som licenspartner (”förmedlare”) och avser licenser/användarkonton, molntjänsten Visiba Care samt service (support, drift, förvaltning och underhåll) av tjänsten. Avtalet består av både leverantörens (Atea) och underleverantörens (Visiba Group AB) standardiserade avtalsvillkor (exempelvis ”Allmänna villkor” från Visiba Group) samt den underliggande offerten från Visiba Group AB samt serviceavtal.

Avtalet saknar helt villkor avseende informationssäkerhet och sekretess. Avtalet saknar även villkor som reglerar säkerhetsbrister, ansvar kring dessa och hur de ska avhjälpas (villkoren är i princip uteslutande inriktade mot användningen av tjänsten och dess tillgänglighet). Det saknas villkor där licenspartnern/leverantören ansvarar för underleverantörens prestation (vilket är brukligt).

Avseende rollerna för leverantör och underleverantör blandas begreppen i de olika delarna av avtalet där definitionen från Ateas del av dokumentationen, till viss del motsägs av definitionen från de delar av Visiba Groups del av dokumentationen.

De allmänna villkoren innehåller en generell begränsning avseende skadestånd på en miljon kronor samt att anspråk måste framläggas inom 90 dagar.

Vidare uppges att leverantören (Atea) ansvarar för att driften av tjänsten (inkluderat support, underhåll och liknande) men ändå inte behandla några personuppgifter på uppdrag av kunden (regionen). Personuppgiftsbehandlingen uppges endast ske av underleverantören (Visiba Group AB) och detta ska regleras i personuppgiftsbiträdesavtal. I övrigt innehåller inte avtalet någon koppling, hänvisning eller liknande till det specifika personuppgiftsbiträdesavtalet.

<u>Dokumentation, personuppgiftsbiträdesavtal</u>
Vi har också tagit del av PuB-avtal mellan Region Örebro län (personuppgiftsansvarig) och Visiba Group AB (personuppgiftsbiträde) daterat den 15 maj 2019, som enligt avtalet avses digitala vårdmöten. Detta avtal hänvisas av nämnden vara det som ska gälla som personuppgiftsbiträdesavtal för användningen av Visiba Care.

Avtalet innehåller i allt väsentligt sedvanliga villkor och de regleringar som krävs enligt GDPR, såsom specifika instruktioner för vilka personuppgifter som får behandlas, lagringstider, krav på säkerhetsåtgärder, krav på sekretessförbindelse för biträdets personal och konsulter, hantering av incidenter, användningen av underbiträden samt rutiner för radering eller återlämning av data när behandlingen upphör. Några särskilda iakttagelser görs dock:

- I avtalet ska namn på tillhörande tjänsteavtal samt datum för dess undertecknande anges. I det aktuella PuB-avtalet är detta fält tomt.

- I avtalet hänvisas till ”Huvudavtalet” och ”Tjänsteavtalet” men det definieras inte vilket avtal det är. Överlag är det tydligt att PuB-avtalet är avsett att vara en bilaga till ett annat avtal och är strukturerat utifrån det.

- När behandlingen avslutas ska personuppgifterna antingen raderas eller återlämnas, utifrån regionens instruktioner, och därefter raderas i samtliga system inom 30 dagar, om inte lagstiftning kräver fortsatt lagring. Det framgår dock inte hur återlämning av data praktiskt ska genomföras.

- Avtalet innehåller även bestämmelser om uppföljning och kontroll. En extern granskning ska genomföras vart tredje år och tillgängliggöras för regionen. Regionen har även möjlighet att genomföra egna revisioner eller låta en utsedd revisor göra detta, varvid Visiba ska tillhandahålla nödvändig dokumentation och åtkomst.

- Avtalet ställer också krav på att Visiba vidtar tekniska och organisatoriska säkerhetsåtgärder som är lämpliga utifrån efter behandlingens art och risker. Det är dock inte tydligt i avtalet om det är PuA eller PuB som avgör vad som kan anses vara en lämplig nivå.

Intervju

Vid intervjuer beskrivs att Visiba Care är Region Örebro läns primära plattform för digitala vårdmöten. Vidare beskrivs att nämnden genomför löpande avstämningar och affärsmöten med Visiba Group AB som del av uppföljningen av tjänstens funktion och användning. Dock kan de intervjuade inte påminna sig att frågor kopplat till informationssäkerhet, sekretess och liknande har varit aktuella. Avstämningarna har inte dokumenterats på ett sätt som medger att PwC kunnat ta del av eventuell dokumentation under denna granskning.

Under intervjuer beskrivs att Atea endast är licenspartner och ”mellanhand” och därför inte på något sätt behandlar personuppgifter eller liknande för regionens räkning. Vid vår invändning att detta upplägg inte stämmer överens med hur avtalet är formulerat har vi inte kunnat få svar på varför skrivningarna i avtalet inte stämmer överens med hur tjänsten i praktiken levereras.

Platform24

Dokumentation

PwC har tagit del av ”Avtal om Kundens användning av Ineras Tjänster”, undertecknat den 7 maj 2018. Av avtalet framgår att regionen köper någon form av tjänst av Inera. Dock är det inte ifyllt i avtalet vilken tjänst som avses, vilket medför att det inte framgår vad avtalet avser. Det aktuella avtalet reglerar

övergripande frågor, och för mer specifika villkor hänvisas till tjänstespecifika bilagor på Ineras hemsida. Eftersom det inte framgår vilken eller vilka tjänster som avtalet avser, är det dock inte möjligt att veta vilka tjänstespecifika villkor som gäller. På Ineras hemsida[12] finns totalt 44 dokument som avser tjänstespecifika villkor, varav flera skulle kunna avse digitala vårdmöten/videomöten.

Vidare framgår att Ineras PuB-avtal 1 reglerar personuppgiftsbehandlingen för Kundens räkning när tjänster som behandlar personuppgifter används, och att regionen är skyldigt att följa Ineras PuB-avtal 1 vid användning av sådana tjänster. Inom ramen för denna granskning har inte nämnden kunnat lämna ut det aktuella PuB-avtalet (varken i signerad eller osignerad form). På Ineras hemsida, där samtliga avtalsdokument är samlade, har vi inom ramen för denna granskning inte kunnat återfinna dokumentet *PuB-avtal 1*. Vid en sökning på internet går det dock att återfinna ett sådant dokument.

Utifrån bakgrunden att det varken går att verifiera vilket avtal eller vilka villkor som gäller för den specifika användningen av Platform24, eller vilket personuppgiftsbiträdesavtal som är tillämpligt, bedömer vi att det inte är möjligt att utvärdera avtalsvillkoren lämplighet eller lagefterlevnad.

Intervju

Vid intervjuer beskrivs att Platform24 används som Region Örebro läns digitala ingång för vårdkontakter. Tjänsten köps och tillhandahålls via Inera, som anges vara regionens avtalspart. Nämnden uppgav att uppföljning sker genom Inera och att regionen inte själv förfogar över riskanalys eller tillhörande tekniska underlag. Platform24 uppgavs vara ett underbiträde till Inera i avtalsrelationen.

Vid intervjuer framhålls även att utifrån att Inera är ett bolag som ägs av kommuner och regioner tillsammans, det vill säga i någon mån regionens eget bolag, litar man på att Inera gör rätt.

Bedömning

Finns ändamålsenligt tjänste- och personuppgiftsbiträdesavtal med leverantören av tjänsten?

Delvis.

Avseende Visiba Care bedömer vi att PuB-avtalet i allt väsentligt följer kraven i GDPR. Avtalet reglerar behandling enligt dokumenterade instruktioner (inklusive Bilaga 1), begränsar biträdets handlingsutrymme till PuA:s instruktioner, ställer krav på sekretess, anger tekniska och organisatoriska säkerhetsåtgärder samt incidentrapportering med kort frist, innehåller villkor för underbiträden med underrättelse och invändningsrätt, reglerar radering/återlämning vid avtalets upphörande samt ger PUA rätt till information, revision och inspektion. Samtidigt är hanteringen vid avtalets upphörande inte fullt ut specificerad. Även om avtalet anger att personuppgifter ska raderas eller återlämnas inom 30 dagar,

[12] https://www.inera.se/kontakta-oss/avtal-bestallning-anslutning/ineras-kundavtal/dokument-i-kundavtalet/#section-15981, 2026-03-13.

saknas i Bilaga 1 en konkret beskrivning av hur återlämning ska ske mellan parterna, vilket bör förtydligas.

Däremot är det problematiskt att tjänsteavtalet brister avseende tydlighet och att säkerhet i princip inte alls regleras. Bristen blir ännu större i ljuset av att det helt saknas en avtalsmässig koppling mellan tjänsteavtalet och personuppgiftsbiträdesavtalet. När avtalen är separerade som de är i detta fall, och endast genom hänvisningar hänger ihop, 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. Det är även i sammanhanget olämpligt med en tidsgräns om 90 dagar för skadeståndsanspråk eftersom det inte är säkert att en incident och/eller skada upptäcks inom den tidsramen.

Utifrån att beskrivningen av hur tjänsten levereras, och hur avtalet är skrivet skiljer sig åt är det svårt att bedöma ändamålsenligheten avseende tjänsteavtalet. Så som avtalet är skrivet, att leverantören (Atea) ska leverera driften av tjänsten, inklusive support, till regionen bedömer vi det som osannolikt att leverantören inte skulle behandla några personuppgifter som regionen ansvarar för. Det är exempelvis svårt, om inte omöjligt, att exempelvis ge support om supportpersonalen inte kan se få åtkomst till vårdpersonalen skärmbild eller kunna läsa loggar i systemet. Båda exemplen innebär behandling av personuppgifter (tillhörande både patienter, anhöriga och vårdpersonal). I ett sådant fall vore det sannolikt att leverantören Atea utgör ett personuppgiftsbiträde och därmed är det obligatoriskt med ett personuppgiftsbiträdesavtal mellan regionen och Atea. Det är också viktigt med ett sådant avtal för att skydda de uppgifter som Atea i ett sådant fall hade behandlat.

Dock uppges vid intervjuerna att Atea endast är en mellanhand och att det är Visiba Care är den leverantör som utför tjänsterna och behandlar personuppgifter och sekretessbelagda uppgifter. Är beskrivningen korrekt innebär det istället att avtalen är inkorrekta och inte speglar den faktiska situationen, vilket tyder på att användningen av Visiba Care inte sker under kontrollerade former i relation till leverantören.

Sammantaget gör vi bedömningen, avseende tjänsteavtalet för Visiba Care, att siatuationen är oklar och att verksamheten inte har kunskap och kontroll över relationen till leverantören. Det innebär betydande risk för att uppgifter inte är skyddade på det sättet som nämnden har utgått ifrån, samt att det vid fel eller brister från leverantören, kan vara svårt att utkräva ansvar.

För Platform24 har vi inte kunnat bedöma avtalsvillkoren eftersom det inte går att verifiera vilka avtal som är gällande. Det är dock en brist i sig att ansvarig verksamhet inte med enkelhet kan identifiera gällande avtal, och att dessa är fullständiga och uppdaterade. Det gör ingen skillnad att det är Inera som är leverantör eftersom regionen fortfarande har samma ansvar utifrån både GDPR, OSL och CSL att säkerställa att kraven på integritet och säkerhet följs.

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 den personuppgiftsansvarige är skyldig att föra ett register över sina behandlingar av personuppgifter. Syftet med registret är för att PuA ska kunna uppfylla sin ansvarsskyldighet, och underlätta tillsyn.[13] Genom registret får organisationen också en tydlig översikt över vilka personuppgifter som behandlas, hur de används och av vilka parter. Detta underlättar för organisationen att ha kontroll över behandlingarna och att identifiera eventuella risker och brister.

Enligt GDPR, art.30.3 ska registret över personuppgiftsbehandlingar ska upprättas skriftligen, det behöver vara tillgängligt i elektroniskt format[14] och hållas uppdaterat. Registret ska innehålla namn och kontaktuppgifter för den personuppgiftsansvarige, 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 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

Dokumentation
Som underlag till revisionsfråga 3 har en anmälningsblankett för registerförteckning, “Visiba Care 251127”, delats. Av blanketten framgår att registrering av en behandlingsaktivitet (exempelvis hantering av personuppgifter i ett visst it-system) sker genom att ansvarig fyller i ett formulär som därefter registreras av dataskyddsombudet (DSO), och att formuläret kan lämnas till DSO via webb eller post. Blanketten saknar fält för att ange hur länge personuppgifter lagras. I övrigt omfattar blanketten uppgifter som ska ingå i en registerförteckning enligt artikel 30 GDPR.

I den registerförteckning för Visiba Care som PwC tagit del av anges att det inte finns några mottagare av personuppgifter. För Pexip och Platform24 har ingen registerförteckning delats med PwC. Dataskyddsombudet har via e-post uppgett att det inte finns någon registrerad behandlingsaktivitet för dessa två system. Vidare uppger Dataskyddsombudet att anmälningsblanketten utgör själva förteckningen för Visiba Care. Dataskyddsombudet uppgifter via e-post att behandlingsregistret inom

[13] Skäl 82, GDPR.
[14] https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/fora-register-over-behandling/#:~:text=Register%20%C3%B6ver%20behandlingar%20ska%20uppr%C3%A4ttas%20skriftligen%2C%20vara%20tillg%C3%A4ngliga%20i%20elektroniskt%20format%20och%20h%C3%A5llas%20uppdaterade.%20P%C3%A5%20beg%C3%A4ran%20ska%20registret%20g%C3%B6ras%20tillg%C3%A4ngligt%20f%C3%B6r%20IMY., 2026-03-14.

Region Örebro län förs manuellt genom att blanketterna sätts i pärmar som förvaras i ett skåp och att det inte finns något digitalt behandlingsregister.

Intervjuer
De inledande intervjuerna indikerar bristande kännedom om registerförteckningen (behandlingsregistret) och dokumenterade behandlingsaktiviteter för Visiba Care, Pexip och Platform24; intervjupersoner uppgav att de inte kände till förekomsten av ett behandlingsregister.

Bedömning

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

Nej.

PwC:s bedömning är att personuppgiftsbehandlingar kopplade till digitala vårdmöten inte är korrekt införda i regionstyrelsens registerförteckning. I registerförteckningen saknas helt personuppgiftsbehandlingarna som sker i Pexip och Platform24. I det delade underlaget för registerförteckning av Visiba Care anges att det saknas mottagare av personuppgifter. Detta bedöms vara felaktigt eftersom tjänsten är en molntjänst och Visiba Care därmed är personuppgiftsbiträde och mottagare av personuppgifter; i det PuB-avtal som är upprättat mellan Region Örebro län och Visiba Care omnämns även flera underbiträden.

Utöver ovan bedömning bedömer vi även att faktumet att registerförteckningen förs analogt är bristfälligt. Det är inte ett explicit krav i GDPR att registret ska föras i elektronisk form, men för att regionen ska kunna efterleva reglerna om ansvarsskyldighet och underlättande av tillsyn behöver det vara i elektronisk form (se not. 14). Den analoga hanteringen medför också risk för att övriga registrerade behandlingsaktiviteter inte hålls uppdaterade och korrekta i enlighet med lagkrav, och försvårar att, vid förfrågan från tillsynsmyndighet, snabbt och fullständigt kunna tillhandahålla förteckningen.

Tjänsteuppföljning: efterlevnad av sekretess och dataskydd

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

Utgångspunkter
Uppföljning på olika sätt är nödvändig för att säkerställa att Region Örebro län följer 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. Ett direkt krav finns i lagen om informationssäkerhet i samhällsviktiga och digitala tjänster, där en årlig, övergripande uppföljning krävs. Krav på uppföljning framgår även av GDPR: den personuppgiftsansvarige får endast anlita biträden som ger ”tillräckliga garantier” för att den enskildes integritet skyddas. EDPB har i vägledning klargjort att detta är en kontinuerlig förpliktelse som behöver följas upp, till exempel genom revisioner och inspektioner. Enligt OSL ska utlämnande av sekretessbelagda uppgifter (vilket ofta sker vid användning av molntjänster) föregås av en lämplighetsbedömning som påverkas av aktuella förhållanden. Det innebär att uppföljning behöver ske för att säkerställa att de förhållanden som den initiala lämplighetsbedömningen grundade sig på fortfarande gäller. Ett indirekt krav finns i kommunallagen, som anger att nämnden ska se till att verksamheten följer gällande regler och har en tillräcklig intern kontroll. För att uppfylla dessa krav i praktiken är uppföljning nödvändig. Att genomföra kontinuerlig uppföljning är således avgörande både för att minimera risker och säkerställa att systemen är tillräckligt säkra, och för att skydda enskildas integritet i enlighet med gällande lagkrav.

Iakttagelser

Dokumentation

Erhållna underlag visar att uppföljning av Platform24, som tillhandahålls Region Örebro län via Inera och 1177, sker genom Ineras taktiska/operativa forum för 1177 symtombedömning och hänvisning (1177 Direkt). Forumet hålls månadsvis och Inera upprättar agenda och mötesanteckningar; mötesinbjudningar, agendor och anteckningar har delats med PwC. Enligt agenda har bland annat riskanalys avseende invånare med skyddade personuppgifter behandlats.

För Visiba Care har nämnden visat en mötesinbjudan till ett kort uppföljningsmöte. Enligt uppgift genomförs avstämningar några gånger per år, men mötesanteckningar upprättas inte. Avseende Pexip uppges att uppföljningsmöten och utbildningsdagar för kompetenshöjning genomförs och deltagande vid Pexip-arrangerade Nordic User Forum och Regiondagen har styrkts av dokumenterade underlag. Inget underlag gällande uppföljning av tjänst initierat av nämnden har uppvisats.

Intervjuer

Vid intervjuer uppges att uppföljning av de digitala vårdtjänsterna sker löpande och på olika sätt beroende på leverantör. För Visiba Care beskriver nämnden att man har regelbundna avstämningar och affärsmöten med leverantören flera gånger per år, även om sådana möten sällan dokumenteras i form av mötesanteckningar.

För Platform24 beskrivs att uppföljning sker inom ramen för Ineras taktiska och operativa forum för 1177 Direkt, vilket enligt uppgift hålls månadsvis och där Inera ansvarar för att ta fram agenda och föra mötesanteckningar.

För Pexip uppgav nämnden att uppföljningsmöten genomförs och att utbildningsdagar anordnas för kompetenshöjning kopplat till tjänstens användning.

Vid intervju bekräftas att ingen uppföljning av tjänst i form av fysisk revision eller skrivbordsrevision för att säkerställa att leverantören uppfyller de krav som avtalats mellan parterna har ägt rum. Enligt uppgift i intervju sker det ingen formell intern uppföljning gällande användning av tjänsterna för att säkerställa att

det brukas på korrekt och angivet sätt. Man uppger att möten kring användning av system sker, men då mer reaktivt utifrån ett problem som uppstått.

Bedömning

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

Nej.

Utifrån intervjuer och erhållen dokumentation är PwC:s samlade bedömning att tjänsterna inte har följts upp på ett ändamålsenligt sätt avseende skydd av sekretessbelagda uppgifter och personuppgifter, främst eftersom det saknas tillräckligt och ändamålsenligt dokumenterat underlag som visar att sådan uppföljning genomförs. För Platform24 finns viss dokumentation via Ineras månadsvisa forum (agendor och mötesanteckningar), men för Visiba Care har endast en mötesinbjudan uppvisats utan anteckningar och för Pexip har inget styrkande underlag delats, utöver deltagande på Nordic User Forum samt Regiondagarna. Sammantaget saknas dokumentation som visar att uppföljning sker på ett sätt som säkerställer och verifierar skyddet av sekretessbelagda uppgifter och personuppgifter. Revisionsfrågan besvaras därför nekande.

Intern styrning för digitala vårdmöten: 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. Av samma skäl är det också viktigt att medarbetare och användare har tillräckligt goda kunskaper avseende relevant cyber- och informationssäkerhet i allmänhet för att exempelvis kunna upptäcka incidenter.

Enligt cybersäkerhetslagen[15] ska organisationen utöva grundläggande praxis för cyberhygien samt säkerställa att medarbetare har tillräcklig kunskap och kompetens för att kunna hantera information och informationssystem på ett säkert sätt.[16]

Det framgår även av MSB:s (idag MCF) 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.[17]

Iakttagelser

Dokumentation

Enligt det delade underlaget ”Ansvar och säkerhet vid digitala möten” (2022) omnämns inte Platform24 som tjänst. Dokumentet reviderades senast 2022. Enligt dokumentet ska uppdateringar ske regelbundet med beaktande av författningsändringar, dock minst vart fjärde år, och regiondirektören utser ansvarig för genomgången.

I underlaget anges att regionen tillhandahåller Skype för företag (under avveckling), Visiba Care, Pexip och Teams (Microsoft Office 365), och att det är innehållet som ska hanteras, diskuteras och delas som avgör vilket mötesverktyg som bör användas. Riktlinjen innehåller inte instruktioner, handledningar eller tekniska beskrivningar för de olika verktygen, utan hänvisar i generella termer till att det kan finnas rutiner eller liknande dokument för specifika verktyg, utan uttryckliga hänvisningar till sådana dokument. Underlaget anger att vid digitala möten ska alla deltagare vara igenkända och att varje part ska kontrollera sin fysiska mötesmiljö, exempelvis att dörrar är stängda. Det anges vidare att Visiba Care uppfyller kraven på kryptering och säker identifiering av patient och vårdpersonal genom elektronisk ID-handling, att Pexip saknar möjlighet till fildelning och att chatten inte lagras i server eller loggar, medan chatt och dokument/filer lagras i molnet vid användning av Teams. Dokumentet beskriver inte hur chatt eller annat systemgenererat material lagras eller gallras.

Enligt delat underlag finns för Platform24/Clinic 24 ett styrande dokument, ”1177 direkt/clinic 24 – övergripande rutiner/riktlinjer” (2023). Det finns ingen hänvisning till detta dokument i ”Ansvar och säkerhet vid digitala möten”, utöver en generell upplysning om att det kan finnas andra riktlinjer. I ”1177 direkt/clinic 24 – övergripande rutiner/riktlinjer” anges arbetsinstruktioner för vårdgivaren om hur systemet används. Dessa arbetsinstruktioner berör inte informationssäkerhet på någon djupare nivå.

Det delade underlaget “Rutin digitala vårdmöten och patienter med skyddade uppgifter” från 2019, som enligt beteckning är en tjänsteanteckning, beskriver hur patienter med skyddad identitet ska ges rätt förutsättningar för beslut om digitalt vårdmöte, istället för fysiskt besök. Av rutinen framgår att patienten ska informeras om att ett mobiltelefonnummer behöver registreras i Visiba Care vid bokning, och att numret då kan ses av alla användare i Visiba Care inom Region Region Örebro län. Om patienten inte

[15] 2 kap. 3 §.

[16] Proposition 2025/26:28, Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag, s. 95.
[17] Vägledning: Säkerhetsåtgärder i informationssystem, Publikationsnummer: MSB2032 – reviderad november 2023, s.33–34.

vill att dennes namn ska synas kan valfri text anges i för- och efternamnsfältet. Vidare krävs mobilt BankID för att genomföra digitala vårdmöten. Eftersom det delade underlaget är betecknat som en tjänsteanteckning är det oklart till vilken grad informationen är etablerad och kommunicerad inom organisationen.

Intervjuer

Vid intervjuer uppges att riktlinjer för digitala vårdmöten finns på intranätet och beskriver hur möten ska genomföras och hur tjänsterna ska användas. Det uppges att informationen om vad som är tillåtet i Teams är tydlig, medan begränsningar avseende Pexip inte framgår på motsvarande sätt. Pexip uppges rekommenderas vid hantering av skyddade uppgifter eftersom tjänsten tillhandahålls lokalt installerat. Det uppges att BankID inte är aktiverat i Pexip och att säker identifiering därmed inte sker i tjänsten. Det uppges vidare att det kan förekomma, eller inte kan uteslutas, att läkare skickar länkar till Pexip-möten till patienter via 1177.

Vid intervjuerna uppges osäkerhet kring om riktlinjerna för digitala vårdmöten tas upp i introduktionsprogrammet för nyanställda. Det uppges att nyanställda ska genomföra en kurs via en plattform, men att det råder osäkerhet kring hur kursdeltagandet följs upp och om genomförande kan verifieras. Intervjupersonerna uppger att det främst finns övergripande rutiner, exempelvis kopplade till distansarbete, och att verksamheten inte har en klar bild av hur efterlevnad säkerställs. Enligt uppgift ligger ansvaret för att medarbetare tar del av rutinerna på respektive linjechef. Det uppges att ett tidigare styrdokument för digitala vårdcentraler togs fram, att medarbetare som deltog i digital mottagning signerade att de tagit del av dokumentet, och att detta därefter användes som grund för riktlinjerna.

Intervjupersonerna uppger att signeringskrav möjligtvis inte längre tillämpas och att efterlevnad i stället faller under sekretess och tystnadsplikt. Det uppges att en informationssäkerhetsutbildning genomfördes för några år sedan, men att det råder osäkerhet om alla berörda medarbetare genomfört utbildningen. Det uppges även att ett IT-introduktionsprogram finns inom hälso- och sjukvården, men att det är oklart om informationssäkerhet ingår och vad programmet omfattar. Inför införandet av 1177 Direkt uppges att behov av utbildningsinsats för digital patientmottagning identifierades, och att kunskapsnivån inom området då uppfattades som omoget, vilket resulterade i en övergripande riktlinje med exempelvis krav på ordning i rummet vid distansarbete och videomöten med patienter.

Bedömning

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

Delvis

PwC bedömer att interna regler, rutiner och vägledning delvis finns, men inte i en sådan omfattning eller detaljnivå att de samlat reglerar och stödjer användningen av digitala vårdmöten. Den övergripande riktlinjen ”Ansvar och säkerhet vid digitala möten” saknar verktygsspecifika instruktioner, hänvisar inte uttryckligen till kompletterande dokument och omfattar inte Platform24/1177, samtidigt som begränsningar för Pexip inte framgår tydligt. Det råder osäkerhet kring om och hur riktlinjerna tas upp i

introduktion och utbildning samt hur efterlevnad verifieras. Det råder osäkerhet kring den utbildning som ges nyanställda samt hur eventuellt utbildning följs upp.

Därutöver, eftersom riktlinjerna delar upp användningen utifrån typ av personuppgift (icke känsliga, känsliga, sekretessbelagda), bedöms personal behöva tydlig och praktisk vägledning för att avgöra vad som utgör en känslig och/eller sekretessbelagd personuppgift, då detta i praktiken inte är självförklarande.

Information om personuppgiftshantering 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 principerna i GDPR är att behandlingen ska ske öppet, vilket bland annat innebär att registrerade har rätt att få veta hur 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. Lättillgängligt innebär exempelvis att informationen inte ska behöva letas upp eller sökas efter och ges på ett sätt som är anpassat för situationen. Klart och tydligt språk innebär bland annat att språket ska vara så enkelt som möjligt och anpassat till målgruppen.[18]

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. 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.[19][20] Även om integritetspolicyn inte ändras avsevärt, är det ändå rekommenderat att ge de registrerade tydliga påminnelser om policyn och var den kan hittas.[21]

[18] https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/de-registrerades-rattigheter/, 2026-02-25

[20] Riktlinjer om öppenhet och information till registrerade, s17. 17/SV
[21] IBID, s18.

Iakttagelser

Dokumentation
Utdrag ur systemflöden och skärmbilder från 1177 visar att patienter, vid inloggning, möts av texten ”Genom att fortsätta godkänner du våra användarvillkor” med länk till användarvillkoren samt en länk ”läs mer om hur vi behandlar dina personuppgifter” som leder till information om Region Örebro läns personuppgiftsbehandling. På 1177.se finns även en generell information avseende personuppgiftsbehandling.

Informationen på regionens hemsida innehåller bland annat beskrivning av personuppgiftsansvarig, hur och för vilket syfte uppgifterna behandlas, hur länge personuppgifterna sparas, var uppgifterna behandlas, mottagare av personuppgifter från regionen, de registrerades rättigheter samt hur klagomål an göras. Samtliga beskrivningar av behandlingen av personuppgifter är översiktlig.[22] Bland annat beskrivs mottagare av personuppgifter översiktligt, utan att namnen på de faktiska mottagarna eller kategorier av mottagare anges. Lagringstid beskrivs på en övergripande nivå och att det avgörs av vad för personuppgift som samlas in och med stöd av vilken rättslig grund. Vissa uppgifter uppges sparas för all framtid medan andra uppgifter raderas så snart de inte längre behövs. Det saknas uppgifter om huruvida tredjelandsöverföring sker men det anges att det kan ske. Det beskrivs att man åtar sig att oavsett geografisk plats för behandling av personuppgifter, alltid vidta alla rimliga legala, tekniska och organisatoriska åtgärder för att säkerställda skyddsnivå.

Vid inloggning via Visiba Care hemsida för Region Örebro län ges informationen via ett dokument som benämns Personuppgiftspolicy. Informationen i denna policy är inte likalydande med den information som finns i Hantering av Personuppgifter på regionens hemsida. Policyn är inte daterad men innehåller specifika beskrivningar av exempelvis vilka personuppgifter som samlas in, syftet med behandlingarna samt mottagare av personuppgifterna. Policyn innehåller också en felaktig hänvisning till Datainspektionen (bytte namn till IMY 2021).

Intervju
Vid intervjuer uppges att patienter informeras om behandlingen av personuppgifter i samband med digitala vårdmöten, framför allt genom 1177-flödet och via användarvillkor som godkänns vid inloggning, med hänvisningar till regionens information om personuppgiftsbehandling. Det uppges vidare att Pexip framför allt används för videokonferenser mellan vårdgivare, och att det är oklart om patienter informeras om att deras personuppgifter kan komma att behandlas i digitala möten där de själva inte är närvarande. Flera intervjuade uppger att de inte varit delaktiga i att ta fram informationsgivningen och kan inte bekräfta vilken typ av information som lämnas inom ramen för Pexip eller om anhöriga informeras när deras uppgifter behandlas.

[22] Hantering av personuppgifter Hantering av personuppgifter • regionorebrolan.se

Bedömning

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

Delvis.

PwC bedömning är att patienter och anhöriga delvis informeras på ett sätt som sammantaget uppfyller kraven i gällande lagstiftning.

Informationen på regionens hemsida är skriven på ett relativt lättförståeligt sätt, den är tillgänglig via startsidan och på rubriknivå motsvarar innehållet den lagstadgade miniminivån av information. Däremot bedömer vi att information överlag är för övergripande för att informationen ska möta den rekommenderade graden av tydlighet och specificering. Att ge övergripande information kan vara godtagbart, om det också ges kompletterande och mer specifik information. Vi bedömer det som svårt för en patient, och ännu svårare för en anhörig, att läsa informationen, och kunna förstå och förutse hur deras personuppgifter behandlas (vilket är syftet med kravet på att ge information). Exempelvis kan det förtydligas för vilka syften personuppgifter behandlas (på kategorinivå) och hur länge de sparas. Informationen avseende överföring till tredje land är inte heller tillräckligt specifik i enlighet med GDPR art. 13.1 (f). Exempelvis bör vilka länder som eventuell överföring ske till anges, samt med vilket rättsligt stöd överföringen sker. Informationstexten saknar också helt beskrivning av vilka uppgifter från anhöriga som kan behandlas och på vilket sätt.

Avseende den information som ges vid användning av Visiba Care är det positivt att informationen är relativt specifik. Däremot är det uppenbart att informationen är inaktuell, till viss del felaktig och det saknas också kontaktuppgifter till dataskyddsombudet.

Samlad bedömning

Utifrån genomförd granskning är vår samlade bedömning att hälso- och sjukvårdsnämnden i Region Örebro län *inte helt* säkerställt att digitala vårdmöten bedrivs på ett ändamålsenligt, lagenligt och informationssäkert sätt. De identifierade bristerna återfinns inom samtliga sex granskningsområden och visar att nämnden behöver utveckla sin riskhantering inom området, säkerställa ändamålsenliga och uppdaterade avtal samt allmänt sammanhållet, systematiskt och dokumenterat arbetssätt för att uppfylla krav enligt GDPR, offentlighets- och sekretesslagen samt god intern kontroll. Sammantaget medför detta en förhöjd risk för bristande regelefterlevnad och ett otillräckligt skydd av sekretessbelagda uppgifter och känsliga personuppgifter.

Den mest betydande svagheten rör avsaknad av genomförda och uppdaterade riskanalyser, konsekvensbedömningar enligt GDPR och lämplighetsbedömningar enligt OSL, såväl inför som under användning av tjänsterna. I kombination med en bristfällig avtalsstruktur blir ansvar, roller och skyddsnivåer oklara i praktiken. Tjänsterna följs inte heller upp på ett systematiskt eller dokumenterat sätt, vilket ytterligare försvagar nämndens kontroll över hantering av sekretessbelagda uppgifter och personuppgifter.

De aktuella personuppgiftsbehandlingar är inte korrekt införda i den registerförteckning som krävs enligt artikel 30 GDPR. Därtill förs behandlingsregistret genom manuell hantering i fysiska pärmar, vilket medför risk för bristande transparens och svårigheter att visa en aktuell registerförteckning vid tillsyn.

Avseende instruktioner för användning av tjänsterna och allmän utbildning kring informationssäkerhet/digital informationshantering finns viss styrning på plats, men inte i sådan omfattning eller detaljnivå att de reglerar och stödjer användningen av digitala vårdmöten.

Granskningen visar även att det inte kan säkerställas att patienter och anhöriga får fullständig och lagenlig information om hur deras personuppgifter behandlas vid digitala vårdmöten.

Sammanfattningsvis behöver hälso- och sjukvårdsnämnden i Region Örebro län förstärka arbetet inom alla sex granskningsområden för att säkerställa en säker, strukturerad och lagenlig hantering av digitala vårdmöten. Nämnden uppger att förbättringsarbete pågår, bland annat införande av informationsklassning och riskanalys, med tillhörande årshjul för uppföljning. Detta förändrar dock inte bedömningen, då bristerna är omfattande och innebär betydande risker för otillräckligt skydd av personuppgifter, bristande spårbarhet och otillräcklig regelefterlevnad.

Rekommendationer

Hälso- och sjukvårdsnämnden rekommenderas att:

1. Genomföra ändamålsenliga risk-, konsekvens- och lämplighetsbedömningar för de digitala vårdtjänster där detta är tillämpligt

Nämnden behöver genomföra och dokumentera fullständiga riskanalyser, konsekvensbedömningar enligt GDPR och lämplighetsbedömningar enligt OSL för de digitala tjänster där lagstiftningen kräver det. Eftersom bristerna i dagsläget är så stora behöver dessa analyser och bedömningar genomföras omgående

2. Säkerställa korrekta, fullständiga och uppdaterade avtal.

Nämnden behöver säkerställa att samtliga relevanta tjänste- och personuppgiftsbiträdesavtal är fullständiga, korrekta och återkommande följs upp tillsammans med respektive leverantör. Avtalen behöver även vara lämpliga i relation till vilka uppgifter som behandlas i de aktuella tjänsterna, vilket tydliggörs i samband med rekommendationen i punkt 1.

3. Införa ett digitalt och systematiskt behandlingsregister

Dagens manuella hantering bör ersättas med ett digitalt, strukturerat och kontinuerligt uppdaterat register enligt artikel 30 GDPR, där alla aktuella personuppgiftsbehandlingar dokumenteras och hålls uppdaterade.

4. Följa upp att leverantörerna efterlever avtalade krav

Nämnden bör genomföra regelbunden och dokumenterad uppföljning av att leverantörer uppfyller de krav och åtaganden som avtalats. Ett första steg är att genomföra den uppföljning som redan idag är möjlig i de befintliga avtalen, endast genom begäran av olika typer av dokumentation.

5. Stärka rutiner och utbildning kring användning och digital informationshantering

Rutiner och instruktioner för användningen av de digitala verktygen bör tydliggöras. Även utbildning kring informationssäkerhet och digital informationshantering bör stärkas. Kombinerat med detta behöver det säkerställas att kunskapsnivåerna inom området ges till nya medarbetare samt upprätthålls över tid.

6. Säkerställa fullständig och lagenlig informationsgivning till patienter och anhöriga

Det behöver säkerställas att informationsgivningen enligt GDPR är både korrekt och fullständig, exempelvis genom att utveckla informationen som finns på regionens hemsida.

Sammanfattande bedömningar utifrån revisionsfrågor

Revisionsfråga	Bedömning	
1. Har ändamålsenlig riskanalys, konsekvensbedömning och lämplighetsbedömning genomförts innan implementering?	**Nej** Nämnden har inte gjort eller dokumenterat riskanalys, konsekvensbedömning eller lämplighetsbedömning på fullständigt sätt för någon av de tjänsterna godkända för digitala vårdmöten.	
2. Finns ändamålsenligt tjänste- och personuppgiftsbiträdesavtal med leverantören av tjänsten?	**Delvis** Ändamålsenligt tjänste- och personuppgiftsbiträdesavtal finns delvis på plats.	
3. Är de personuppgiftsbehandlingar som digitala vårdmöten innebär, korrekt införda i regionstyrelsens registerförteckning över personuppgiftsbehandlingar?	**Nej** Personuppgiftsbehandlingar kopplade till digitala vårdmöten är inte fullständigt och korrekt införda i registerförtäckning.	
4. Har tjänsten följts upp på ett ändamålsenligt sätt, avseende skydd av sekretessbelagda uppgifter och personuppgifter?	**Nej** Tjänsterna har inte följts upp på ett ändamålsenligt sätt. Det saknas dokumenterade underlag som styrker att relevant uppföljning genomförs.	
5. Finns interna regler, rutiner och vägledning som reglerar och stödjer användningen av digitala vårdmöten?	**Delvis** Interna regler, rutiner och vägledning finns delvis men inte i sådan omfattning eller detaljnivå att de 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?	**Delvis** Patienter och anhöriga informeras delvis på ett sätt som sammantaget uppfyller kraven i gällande lagstiftning.	

2026-03-20

Rebecka Hansson	Charlotte Arnell
Uppdragsledare	*Projektledare*

Denna rapport har upprättats av Öhrlings PricewaterhouseCoopers AB (org nr 556029-6740) (PwC) på uppdrag av Region Örebro läns revisorer enligt de villkor och under de förutsättningar som framgår av projektplan från den 6 oktober 2025. PwC ansvarar inte utan särskilt åtagande, gentemot annan som tar del av och förlitar sig på hela eller delar av denna rapport.