Granskning av avtalsstyrning och uppföljning av privata vårdgivares informationssäkerhet

Region Norrbotten

April 2023

Kristian Damlin

Charlotte Arnell

Markus Månsson

pwc

Revisionsrapport

Sammanfattning

PwC har på uppdrag av de förtroendevalda revisorerna i Region Norrbotten genomfört en granskning av avtalsstyrning och uppföljning av privata vårdgivares informationssäkerhet. Granskningen syftar till att bedöma om regionstyrelsen säkerställer en ändamålsenlig avtalsstyrning och uppföljning av privata vårdgivares informationssäkerhet samt ifall den interna kontrollen i sammanhanget är tillräcklig. Granskningen syftar även till att säkerställa att regionen uppfyller kommunallagens krav om internkontroll.

Utifrån genomförd granskning är vår samlade bedömning att regionstyrelsen i Region Norrbotten **inte helt** säkerställer en ändamålsenlig avtalsstyrning och uppföljning av privata vårdgivares informationssäkerhet. Vi bedömer att den interna kontrollen **ej** är tillräcklig.

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

Revisionsfrågor	**Bedömning**	
1. Har regionen säkerställt att tillräckliga krav ställs på privata vårdgivare i samband med upphandling utifrån ett legalt, säkerhetsmässigt och affärsmässigt perspektiv?	Delvis	
2. Har regionen implementerat de identifierade kraven på ett ändamålsenligt och effektivt sätt i avtalen med de upphandlade leverantörerna?	Delvis	
3. Följer regionen upp att de avtalade kraven och villkoren följs av leverantörerna på ett ändamålsenligt sätt?	Nej	
4. I det fall avvikelser upptäcks, har regionen ett ändamålsenligt sätt att hantera dessa avvikelser?	Delvis	

Rekommendationer

- Regionstyrelsen bör arbeta för att skapa medvetenhet och kunskap avseende de externa vårdgivarnas betydelse avseende informationssäkerhet, och hur deras agerande och eventuella brister kan påverka regionen.
- Regionstyrelsen bör tydliggöra roller och ansvar för att uppnå en lämplig och ändamålsenlig kravställning utifrån ett informationssäkerhetsperspektiv. Ansvaret och vad de olika rollerna förväntas göra bör beskrivas i regionens styrande- och stödjande dokument.
- Regionstyrelsen bör säkerställa att kravställning, val av kriterier i kvalificering och utvärdering samt avtalsvillkor i större utsträckning präglas av en riskbedömning avseende vilka specifika informationssäkerhetsrisker och vilka informationssäkerhetskrav som behöver hanteras vid upphandling av privat vård.
- Regionstyrelsen bör utveckla avtalsvillkoren vid den här typen av upphandlingar för att öka incitamenten för vårdgivarna att självständigt och proaktivt arbeta för utveckling och förbättring av informationssäkerhet.
- Regionstyrelsen bör utveckla krav och avtalsvillkor på ett sådant sätt att de blir mer tydliga och lättare att följa upp och kontrollera.
- Regionstyrelsen bör etablera arbetssätt för att hantera avvikelser avseende informationssäkerhet.
- Regionstyrelsen bör säkerställa att återkommande systematisk uppföljning av externa vårdgivares informationssäkerhet genomförs.

Innehållsförteckning

Sammanfattning	1
Förkortningar och begrepp	4
Inledning	4
Bakgrund	4
Varför är informationssäkerhet viktigt?	5
Upphandling av vård	6
Syfte och revisionsfrågor	7
Revisionskriterier	9
Avgränsning	10
Metod	10
Granskningsresultat	11
Kravställning vid upphandling	11
lakttagelser	11
Implementering av upphandlingskrav i efterföljande avtal	14
Uppföljning av upphandlingskrav och avtalsvillkor	19
Samlad bedömning	23
Sammanfattande bedömningar utifrån revisionsfrågor	25

Förkortningar och begrepp

GDPR	Den allmänna dataskyddsförordningen
HSL	Hälso- och sjukvårdslag
IVO	Inspektionen för vård och omsorg
LOU	Lag om offentlig upphandling
LOV	Lag om valfrihetssystem
OSL	Offentlighets- och sekretesslag

Inledning

Bakgrund

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

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

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

En betydande del av sjukvården i Sverige bedrivs utanför regionernas organisationer. Detta kan i sin tur innebär att den enda egentliga styrning av denna verksamhet som en region kan utföra, är genom att ställa rätt krav vid upphandling, säkerställa att dessa krav, tillsammans med ändamålsenliga villkor, avtalas om med vinnande leverantörer, därefter följa upp att avtalen följs, samt vid avvikelser vidta ändamålsenliga åtgärder.

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

Det finns ett flertal olika lagstiftningar och föreskrifter som reglerar informationshantering och -säkerhet inom hälso- och sjukvård. I de flesta fall utgår regelverket dock från vårdgivarens ansvar och skyldigheter i olika situationer. Det innebär att Region Norrbotten inte har ett eget, självständigt ansvar för att en upphandlad vårdgivare uppfyller exempelvis dataskyddslagstiftning eller patientsäkerhetslagstiftning.

Däremot har regionen ett uppföljnings- och kontrollansvar, exempelvis utifrån kommunallagens bestämmelser. Man har även ett ansvar som huvudman att kunna erbjuda hälso- och sjukvård i enlighet med hälso- och sjukvårdslagen, vilket innebär både ett ansvar kopplat till kapacitet och förmåga, samt kvalitet. För att kunna efterleva de kraven är avtalen de viktigaste verktygen som regionen har, och hur dessa är skrivna blir därmed avgörande.

Revisorerna i Region Norrbotten har identifierat en risk för att regionen inte ställer tydliga krav på informationssäkerhet i de avtal som tecknas med externa vårdgivare, inte reglerar dessa på ett effektivt sätt i avtalen och inte i tillräcklig omfattning följer upp de krav som ställs.

Varför är informationssäkerhet viktigt?

Information är i de flesta sammanhang mer eller mindre viktigt, och beroende på sammanhang och omständigheter kan den ha ett mycket högt värde (ofta är värdet högre om den innehåller personuppgifter). Information som delas med obehöriga personer, som ändras av obehöriga eller på ett felaktigt sätt, och/eller som inte finns till hands när den behövs kan innebära stora negativa konsekvenser för både en verksamhet och enskilda individer. Informationssäkerhet handlar om att hantera och skydda informationen, oavsett var den finns, på ett sätt så att sådana konsekvenser inte uppstår.

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

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

Om man som organisation väljer att tillgängliggöra information till en extern part, eller möjliggöra tillgång till exempelvis IT-system för en tredje part, behöver samma medvetenhet genomsyra leverantörsstyrning och -uppföljning. Annars är risken att leverantören, exempelvis en vårdgivare, blir en sårbarhet för den överlämnande organisationen.

Upphandling av vård

Region Norrbotten är ansvarig för att tillhandahålla sjukvård enligt HSL. Detta kan göras genom egen regi i någon form, eller upphandlade utförare. Upphandlingarna kan ske genom LOU eller LOV.

Oavsett om en upphandlande myndighet gör en upphandling enligt LOU eller inom ett valfrihetssystem enligt LOV måste de krav och villkor som ska gälla fastställas och annonseras. I en upphandling enligt LOU ska upphandlingsunderlaget annonseras, och de leverantörer som vill konkurrera om uppdraget måste lämna ett anbud senast på ett anvisat datum. Av upphandlingsunderlaget ska det också framgå hur anbuden kommer att utvärderas och rangordnas. Den leverantör som lämnat det mest förmånliga anbudet utifrån den utvärderingsmodell som den upphandlande myndigheten bestämmer, vinner upphandlingen och tilldelas kontrakt.

I ett valfrihetssystem enligt LOV ska förfrågningsunderlaget löpande annonseras. Kontrakt tecknas sedan kontinuerligt med leverantörerna vartefter deras ansökningar blir godkända. Alla leverantörer som lämnar in en ansökan som uppfyller de krav och villkor som framgår av upphandlingsunderlaget ska godkännas, skriva kontrakt och bli leverantör i valfrihetssystemet. Den enskilde väljer sedan en leverantör av de som är anslutna till valfrihetssystemet.

Region Norrbotten bedriver vård både i egen regi och genom att upphandla privata vårdgivare enligt både LOU och enligt LOV. Upphandlad vård enligt LOU avser operationstjänster, där det finns ett ramavtal med flera leverantörer anslutna. Upphandlad vård enligt LOV avser primärvård och omfattar cirka 17 procent av de listade patienterna. Även barn- och ungdomstandvård finns upphandlat enligt LOV, men omfattar en mycket liten del av den totala verksamheten.

Leverantörer av operationstjänster ansluts inte till regionens IT-miljö. Remisser mellan regionen och den externa vårdgivaren skickas med post. Vårdgivare anslutna till LOV ansluts däremot till vissa delar av regionens IT-miljö och system/tjänster.

Syfte och revisionsfrågor

Granskningen syftar till att bedöma om regionstyrelsen säkerställer en ändamålsenlig avtalsstyrning och uppföljning av privata vårdgivares informationssäkerhet samt ifall den interna kontrollen i sammanhanget är tillräcklig. Granskningen syftar även till att säkerställa att regionen uppfyller kommunallagens krav om internkontroll.

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

1. **Har regionen säkerställt att tillräckliga krav ställs på privata vårdgivare i samband med upphandling utifrån ett legalt, säkerhetsmässigt och affärsmässigt perspektiv?**

När varor och tjänster inte produceras av den egna verksamheten, utan köps in från extern part styrs leveransen till största del av de villkor som finns i avtalet mellan upphandlande myndighet och leverantör. Avtalsvillkoren styrs i sin tur av upphandlingsunderlaget och de krav och villkor som framgått där. Möjligheterna till förändrade krav och villkor inom ramen för ingångna avtal är relativt begränsade, av både upphandlingsrättsliga och kommersiella skäl. Detta innebär att det är mycket viktigt att redan vid utarbetandet av upphandlingsunderlaget sätta krav och villkor på en ändamålsenlig nivå för att tjänsten som sedan levereras lever upp till både obligatoriska krav och förväntningar.

Kraven som ställs vid upphandling behöver självklart täcka in flera områden, men för denna granskning fokuseras endast på det legala, säkerhetsmässiga och affärsmässiga perspektiven inom ramen för informationssäkerhet.

Utifrån ett legalt perspektiv behöver kraven innebära att leverantören följer den lagstiftning som finns på området. Regionen behöver också tillförsäkra sig möjlighet att följa upp och kontrollera att leverantören följer lagstadgade krav, för att för egen del kunna leva upp till obligatoriska krav.

Utifrån ett säkerhetsmässigt perspektiv behöver formella säkerhetskrav inkluderas i kravställningen, både de som ställs på leverantören som vårdgivare, och de som ställs på regionen, som ska effektueras genom dess leverantörer. Avseende dessa krav behöver det också säkerställas att regionens IT-miljö och dess funktionalitet samt interna regler och krav inte äventyras genom anslutning eller användning av den upphandlade leverantören.

När det gäller det affärsmässiga perspektivet är detta viktigt att beakta i kravställningen, för att skapa incitament till följsamhet och bästa möjliga lösningar avseende de direkta kraven avseende säkerhet. Avseende just informationssäkerhet är detta extra viktigt eftersom utvecklingen, av både tekniska möjligheter, normer och standarder samt externa hot går snabbt. Det kan exempelvis handla om att kravställa på kontinuerlig utveckling av säkerhetslösningar eller proaktiva åtgärder från leverantören.

Att kartlägga, formulera och prioritera behov och krav inför upphandling är många gånger ett svårt, komplext och omfattande arbete. Inte sällan är en mängd personer och funktioner involverade. För att upphandlingarna ska bli framgångsrika över tid, behövs därför ett systematiskt arbetssätt. Syftet med ett systematiskt arbetssätt är bland annat att säkra upp att alla nödvändiga krav finns med genom att alla relevanta funktioner involveras i upphandlingen, att de beslutsfattare som är ansvariga för upphandlingen även ges möjlighet att ta ansvar för prioritering av krav (som i praktiken ofta innebär en värdering av risker), att utvärderingsmodell och utvärdering återspeglar prioriteringen mellan kraven, och att även uppföljningen av avtal och leverans täcker in alla krav.

2. **Har regionen implementerat de identifierade kraven på ett ändamålsenligt och effektivt sätt i avtalen med de upphandlade leverantörerna?**

För att de krav som ställts i upphandlingen ska kunna realiseras krävs effektiva villkor. Med effektiva menas bland annat att villkoren ska skapa incitament för följsamhet från leverantörens sida, de ska skapa förutsättningar för att förändringar och oförutsedda händelser (exempelvis förändringar i lagstiftning under avtalstidens gång), de ska ge möjlighet till en ändamålsenlig grad av insyn och skapa förutsättningar för rationella arbetssätt avseende uppföljning.

I begreppet ligger också att villkoren ska vara skrivna på ett sätt som gör dem tydliga och möjliga att förstå även några år efter att de skrivits. Avtalsvillkoren behöver också innehålla effektiva sanktionsmöjligheter, i det fall leverantören brister i leverans eller utförande. Exempelvis behöver avtalet innehålla sanktioner som utgör tillräckligt starka incitament för leverantören att följa avtalet, men samtidigt behöver sanktionerna vara enkla att administrera och inte leda till bland annat onödiga prisökningar. Sanktionerna behöver också vara praktiskt möjliga att tillämpa, utifrån att regionen kan ha ett starkt beroende av den levererade tjänsten.

3. **Följer regionen upp att de avtalade kraven och villkoren följs av leverantörerna på ett ändamålsenligt sätt?**

Både upphandlingskrav och avtalsvillkor är teoretiska aspekter. För att leveransen ska bli så som förväntat behövs i de allra flesta fall uppföljning av hur arbetet går till, och hur en leverans blev, i praktiken. Detta bör involvera olika typer av uppföljning, både den mer formella avtalsrevisionen, proaktiv uppföljning i form av exempelvis tester, simulerade incidenter och liknande, samt uppföljning av leveranser i efterhand.

Samtidigt behöver uppföljningen ske på ett väl avvägt sätt för att spegla relationen mellan risk och kostnaden för själva uppföljningen. Dessutom behöver själva uppföljningen utföras på ett effektivt och rationellt sätt, och inte ”störa” leverantören på ett oproportionerligt sätt.

Olika områden behöver följas upp på olika sätt. När det gäller informationssäkerhet kan lämpliga metoder vara exempelvis simulerade incidenter, tester av olika slag, samt kontroll att leverantören har olika typer av dokumentation på plats.

4. **I det fall avvikelser upptäcks, har regionen ett ändamålsenligt sätt att hantera dessa avvikelser?**

Att avvikelser sker och upptäcks är egentligen inget konstigt i sig självt, utan är något som i viss utsträckning behöver kalkyleras med. Därför är det viktigt att avvikelserna hanteras på ett riskmedvetet och effektivt sätt. Ett exempel är att det behöver vara tydligt i avtalet vilka konsekvenser olika typer av avvikelser får. Grunden för detta läggs redan under upphandlingsprocessen, när regionen formulerar avtalsvillkor.

Det är också viktigt att avvikelserna används på ett värdeskapande sätt, av både regionen och vårdgivare, så att det kan skapas ett lärande som båda parter kan använda sig av och förbättra sin verksamhet respektive leverans.

Revisionskriterier

Bedömningsgrunderna bildar underlag för de analyser och bedömningar som gjorts i promemorian.

Kommunallag

Kommunallagen ger regionen möjlighet att lämna över utförandet av verksamhet som man är ansvarig för, till andra juridiska personer. Exempel på en sådan är en privat vårdgivare. När ett överlämnande sker till en privat utförare måste dock den överlämnande nämnden kontrollera och följa upp den privata utföraren. Den verksamhetsansvariga nämnden har även ett allmänt ansvar att försäkra sig om att den verksamhet som de ansvarar för följer lagar och regler, oavsett om den utförs av nämnden själv eller är överlämnad till annan utförare.

Hälso- och sjukvårdslag

I lagstiftningen förtydligas att en region får sluta avtal med annan aktör att utföra hälso- och sjukvård. Dock har regionen kvar det yttersta ansvaret som huvudman. Det innebär att man har det yttersta ansvaret för att regionens invånare kan erbjudas den hälso- och sjukvård som de har rätt att få enligt denna lagstiftning. Det innebär i sin tur att det avtal om utförande som tecknas, måste säkerställa regionens kapacitet och förmåga att leva upp till lagstiftningens.

Socialstyrelsens föreskrifter och allmänna råd om ledningssystem för systematiskt kvalitetsarbete

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

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

I föreskrifterna regleras bland annat vad som ska gälla allmänt avseende en vårdgivares informationssäkerhetsarbete (exempelvis ledning av informationssäkerhetsarbete, kontinuitetsarbete och säkerhetskopiering), åtkomst till patientuppgifter, allmänt om hantering av personuppgifter och hur patientjournaler ska struktureras och tas hand om.

Lag och förordning om informationssäkerhet för samhällsviktiga och digitala tjänster

Syftet med lagen och tillhörande förordning är att säkerställa en hög gemensam nivå på säkerhet i nätverk och informationssystem, som samhället är beroende av för en trygg och stabil funktionalitet. Alla branscher och sektorer träffas inte av regelverket, men just hälso- och sjukvård är en av de som omfattas, och anledningen är dess viktiga funktion i samhället.

Regelverket beskriver bland annat att ”leverantörer av samhällsviktiga tjänster”, som kan vara både från offentlig och privat sektor, ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete, att riskanalyser måste göras och att både organisatoriska och tekniska åtgärder måste vidtas för att upprätthålla säkerheten. Det ställs även krav på hur incidenter måste hanteras och rapporteras.

Beprövad erfarenhet och branschkunskap

För vissa delar av frågorna, exempelvis hur avtalsvillkor är utformade och om uppföljning är ändamålsenlig, går det inte att hitta svaren på frågorna i en lagregel eller liknande. Bedömningarna är i stället grundade på den erfarenhet och kunskap av liknande verksamhet och frågeställningar, samt kunskap om vad som anses utgöra ”best practice”, som konsulterna besitter.

Avgränsning

Granskningen omfattar upphandlingar av privata vårdgivare, där avtalen är gällande vid tidpunkten för granskningen.

Granskningen omfattar upphandlingar av privata vårdgivare, där avtalen är gällande vid tidpunkten för granskningen. Vårdgivare verksamma enligt lag om läkarvårdsersättning eller lag om ersättning för fysioterapi, ingår inte i denna granskning.

Metod

Granskningen har genomförts genom att relevanta styrande och stödjande (exempelvis riktlinjer och anvisningar) dokument granskas. Vi har även granskat upphandlingsunderlag och avtal för vårdval, primärvård samt operationstjänster inom öppen- och slutenvård.

Information har inhämtats, genom e-post och vid intervjuer, med följande funktioner;

- Upphandlare
- Upphandlingschef
- Beställarchef
- Informationssäkerhetssamordnare/säkerhetsskyddsstrateg
- Verksamhetschef IT/MT-stöd

De intervjuade har beretts möjlighet att sakgranska rapporten.

För förståelsen används i denna rapport begreppet ”LOV-upphandling” respektive ”LOU-upphandling” för att särskilja de två olika typerna av upphandling, även om de i sin uppbyggnad och funktion skiljer sig en del åt.

Granskningsresultat

Kravställning vid upphandling

Revisionsfråga 1: Har regionen säkerställt att tillräckliga krav ställs på privata vårdgivare i samband med upphandling utifrån ett legalt, säkerhetsmässigt och affärsmässigt perspektiv?

Iakttagelser

Styrande dokument

Regionen har etablerat flera styrande dokument avseende arbetet med informationssäkerhet. Exempelvis finns en övergripande säkerhetspolicy som anger regionens inriktning och värdegrund samt övergripande målsättning i arbetet med informationssäkerhet. I säkerhetspolicyn anges att regionen ska bedriva ett systematiskt säkerhetsarbete i syfte att säkerställa integritet, säkerhet och trygghet för patienter, anställda, förtroendevalda och alla övriga som berörs av regionens olika verksamheter. Detta riktar sig till alla verksamheter som bedrivs i egen regi eller på uppdrag av regionen.

Regionen har även en *anvisning för IT och informationssäkerhet* som beskriver organisation för informationssäkerhet samt styrande principer inom flera områden såsom riskhantering, hantering av tillgångar, åtkomsthantering, fysisk säkerhet och driftsäkerhet. I anvisningen anges även att regionen ska säkerställa att uppdragstagare eller andra som arbetar för eller har slutit avtal med regionen förbinder sig att med lämpliga tekniska och organisatoriska säkerhetsåtgärder skydda informationen som ingår i omfattningen för regionens ledningssystem. I granskningen framgår att organisationen och dess verksamheter ska konkretisera dessa styrprinciper genom att etablera rutiner och arbetssätt som understödjer detta.

Regionen har även etablerat flera styrande och stödjande dokument avseende arbetet med upphandlingar. De styrande dokumenten anger exempelvis övergripande mål och styrande principer. De stödjande dokumenten beskriver exempelvis roller och ansvar under upphandlingsprocessen samt vilka steg som ska genomföras inför och under upphandlingsprocesser. Ett av stegen som ska genomföras inför en upphandling genomförs är att utse en upphandlingsgrupp. Denna grupp ska bland annat ansvara för att utforma kravspecifikation och delta vid utvärdering av inkomna anbud. Gruppen ska bestå av sakkunniga personer från verksamheten och innehålla samtliga kompetenser som krävs för att den samlade kunskapen ska täcka in alla produkter/utrustningar/tjänster som ingår i upphandlingen.

Vi har inom ramen för granskningen inte kunnat se att det finns någon dokumentation som reglerar hur regionen ska säkerställa att ändamålsenliga krav avseende informationssäkerhet ställs i dessa typer av upphandlingar. Exempelvis framgår det inte tydligt tydligt vem som har ansvar att kravställa utifrån ett informationssäkerhetsperspektiv samt vilka perspektiv som särskilt ska beaktas.

Upphandlingsunderlag

Vid genomgång av de upphandlingsunderlag som vi tagit del av inom ramen för granskningen noteras både likheter och skillnader i underlagen avseende kraven ur ett informationssäkerhetsperspektiv. Båda underlagen innehåller krav på att leverantören ska följa de lagar som omfattar deras verksamhet. Detta inkluderar indirekt lagar relaterat till informationssäkerhet såsom lagen om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-direktivet) samt Dataskyddsförordningen (GDPR). I LOU-underlaget är dock skrivningen om att leverantören ska följa lagar som omfattar deras verksamhet författat under rubriken “Kvalitetsledningssystem - Patientsäkerhet”, vilket medför att det finns en viss otydlighet i om all lagstiftning avses eller om det endast är lagstiftning relaterat till kvalitetsarbete och patientsäkerhet som avses. Utöver detta inkluderar båda upphandlingsunderlagen även krav som anger att leverantören ansvarar för eventuella underleverantörers åtaganden (vilket även det inkluderar åtaganden relaterat till informationssäkerhet).

Vid granskning av upphandlingsunderlaget avseende operationstjänster identifieras inga ytterligare specifika krav relaterat till informationssäkerhet. Upphandlingsunderlaget för vårdval primärvård inkluderar, utöver ovan, även krav på sekretess och kontinuitet samt krav på vissa tekniska säkerhetsåtgärder relaterat till exempelvis IT-infrastruktur, autentisering, brandväggar och loggkontroll. En anledning till att det skiljer sig åt avseende kravnivå är att leverantörerna i LOV-upphandlingen kommer åt vissa delar av regionens IT-miljö, vilket inte är fallet för leverantören i LOU-upphandlingen.

Intervjuer

Under intervjuer beskrivs att medarbetare inom olika professioner involveras i arbetet med att etablera upphandlingsunderlagen. Det framkommer även att det är verksamhetsansvarig som avgör om kravställning utifrån ett informationssäkerhetsperspektiv ska inkluderas i upphandlingen. Vidare anges att det i så fall är medarbetare från regionens MT/IT-avdelning som ska involveras i arbetet med att definiera krav relaterat till informationssäkerhet.

Intervjupersoner lyfter dock fram att verksamheten behöver få mer kunskap kring när krav relaterat till informationssäkerhet behöver inkluderas samt varför det är viktigt. Det beskrivs även finnas en generell utmaning med att MT/IT involveras för sent i samband med upphandlingsprocesser då de ibland blir involverade efter att upphandlingen redan är avslutad.

Bedömning

Har regionen säkerställt att tillräckliga krav ställs på privata vårdgivare i samband med upphandling utifrån ett legalt, säkerhetsmässigt och affärsmässigt perspektiv? Svar: Delvis

Vi bedömer att båda de granskade upphandlingsunderlagen direkt eller indirekt innehåller krav relaterat till informationssäkerhet. Detta eftersom båda upphandlingsunderlagen innehåller krav på att leverantören ska efterleva tillämplig lagstiftning. Vidare bedöms det finnas en viss skillnad på nivån av krav som inkluderas i upphandlingsunderlagen. Att upphandlingsunderlaget för LOU-upphandlingen inte innehåller fler specifika krav avseende informationssäkerhet än att följa tillämplig lagstiftning bedöms som en brist. Upphandlingsunderlaget för LOV-upphandlingen innehåller något fler krav avseende informationssäkerhet. Men kraven bedöms dock inte vara heltäckande. Exempelvis saknas tydligt angivna krav gällande systematiskt informationssäkerhetsarbete, processer för riskhantering, hantering av tillgångar samt krav på fysisk säkerhet. Med beaktande av detta bedöms inte kraven i de båda upphandlingsunderlagen vara tillräckliga.

Tillvägagångssättet med att inkludera krav på informationssäkerhet genom att främst ange att leverantören ska följa tillämplig lagstiftning medför vissa risker. Exempelvis innebär det att en potentiell vårdgivares förmåga att följa tillämplig lagstiftning samt hur de tillämpas i eventuell befintlig verksamhet (alternativt hur de planeras att tillämpas), aldrig egentligen prövas innan tilldelningsbeslut/godkännande och därefter avtalsskrivande.

Detta medför i sin tur att kraven avseende informationssäkerhet, som i teorin ställs, i praktiken blir relativt uddlösa. Detta innebär att det finns risk för att regionen tecknar avtal med vårdgivare som inte har förmåga att följa det tecknade avtalet, och inte heller leverera vård enligt de premisser som regionen kravställt på.

Det innebär också en affärsmässig risk för regionen att ingå avtal med parter där regionen inte på förhand har kartlagt deras förmågor tillräckligt. Man riskerar då att hamna i en situation där brister uppdagas och olika typer av sanktionsmekanismer i avtalet behöver aktiveras, eller där avtalet till och med behöver hävas/avslutas.

Allt detta kan leda till merarbete, sänkt vårdkapacitet och kanske till och med kvalitetsbrister för regionen. Utifrån detta resonemang hade det varit önskvärt om det ingick moment kopplat till informationssäkerhet vid kvalificering (LOV) och utvärdering (LOU), exempelvis genom inlämnande av dokumentation som visar hur man efterlever socialstyrelsens föreskrift om journalföring och behandling av personuppgifter.

Implementering av upphandlingskrav i efterföljande avtal

Revisionsfråga 2: Har regionen implementerat de identifierade kraven på ett ändamålsenligt och effektivt sätt i avtalen med de upphandlade leverantörerna?

Iakttagelser

Avtal, vårdval primärvård

Avtalsvillkoren framgår både av huvudavtalet men även av det upphandlingsunderlag/ansökan som kallas Beställning. Avseende informationssäkerhetskrav och villkor framgår de flesta av beställningsdokumentet (se närmare beskrivning under revisionsfråga 1).

Avseende lagstiftning och regionens egna styrande dokument anges att leverantören ska vara väl förtrogen med dessa, samt följa både relevant lagstiftning och regionens styrande dokument. Det förtydligas att de styrande dokumenten ska avse primärvård, men i övrigt förtydligas inte villkoret. Det framgår även att leverantören ska tillämpa Socialstyrelsens föreskrift om ledningssystem för kvalitetsarbete samt ha ett ändamålsenligt system för internkontroll. Detta ska även kunna redogöras för på förfrågan.

Utifrån ersättningsmodellen kan vi inte se att det utgår någon form av mål- eller prestationsinriktad ersättning avseende informationssäkerhet. Vi kan heller inte se att regionen har någon möjlighet att innehålla betalning till vårdgivare, exempelvis i händelse av pågående brist. Däremot har man möjlighet att kvitta ersättning mot vite i förekommande fall.

I LOV-avtalet framgår att om leverantören brister i sin uppfyllelse av avtalet så har regionen rätt att fatta beslut om vite intill dess att bristen är åtgärdad. I avtalet finns ingen fastställd nivå eller modell för vitet, utan det framgår endast att vitet ska vara skäligt i förhållande till felet och inte får överskrida 100 procent av maximal månadsersättning. I beställningsdokumentet anges taket för vite till tio procent av månadsersättningen.

Det framgår även att regionen har rätt att i förtid säga upp avtalet (med den uppsägningstid som regionen bestämmer) om leverantören visar sig till väsentlig del inte uppfylla de krav som uppställs i regelverket för Vårdval Norrbotten. Detta kan exempelvis inträffa om leverantören agerar på sådant sätt att det allvarligt skadat förtroendet för regionen som beställaren och inte vidtar rättelse inom skälig tid efter skriftligt påpekande från regionen.

Enligt avtalet ges regionen rätt att följa upp leverantörens utförande av uppdraget, samt möjlighet till insyn för att möta kommunallagens krav på allmänhetens insyn hos privata utförare. I beställningsdokumentet anges att leverantören ska lämna de uppgifter som regionen behöver för att kontrollera leverantörens säkerhetssystem. Det anges också att regionens revisorer har rätt att inhämta uppgifter. Det är dock oklart om det är uppgifter från leverantören som åsyftas.

Avtal, ramavtal operationstjänster

Avtalsvillkoren framgår av dokumenten administrativa föreskriver, ramavtal samt kontrakt för förnyad konkurrensutsättning.

I avtalet anges att leverantören ska följa samtliga relevanta lagar och föreskrifter samt branschpraxis. Men det används även formuleringar som exempelvis “verksamheten ska drivas utifrån de krav som anges i lagstiftning”. Avseende informationssäkerhet specificeras att för att säkerställa säker identifiering ska patientdatalagen eller motsvarande följas. I övrigt specificeras inga krav eller villkor som avser informationssäkerhet, så som det görs avseende exempelvis vårdhygien. Det anges även att vårdgivaren är personuppgiftsansvarig för personuppgiftsbehandlingar i patientjournaler. I övrigt uppställs inget villkor om att leverantören ska följa GDPR eller kunna visa upp dokumentation som styrker efterlevnad, eller liknande.

När det gäller sekretess anges att leverantören, dess personal och uppdragstagare inte får avslöja konfidentiell information till tredje part. Med konfidentiell information förtydligas att det är sådan information som omfattas av sekretess och tystnadsplikt enligt OSL. Det anges att regeln ska tillämpas som om leverantörens anställda och uppdragstagare hade varit anställda av regionen. I ramavtalet anges att avvikelser ska registreras i ändamålsenligt system. Det framgår inte vilken typ av avvikelser, eller vilka system som avses.

Avseende uppföljning stadgas att avtalet ska följas upp vid behov, men klargörs inte vem som avgör när behov föreligger eller vem som är ansvarig för uppföljning. Avseende tillgång till data (inte ett definierat begrepp i avtalet så det är inte klarlagt vad som avses med begreppet) i samband med uppföljning, begränsar regionen sin egen möjlighet till att tillgången måste följa patientdatalagen eller motsvarande. Däremot anges att regionens revisorer ska ha full tillgång till den information man anser sig behöva för att utföra sitt uppdrag.

Utifrån avtalets ersättningsmodell kan vi inte se att det utgår någon form av mål- eller prestationsinriktad ersättning avseende informationssäkerhet. Vi kan heller inte se att regionen har någon möjlighet att innehålla betalning till vårdgivare, exempelvis i händelse av pågående brist.

Det framgår också att regionen har möjlighet att utfärda vite eller sanktioner om leverantören inte uppfyller åtaganden enligt avtalet eller dess bilagor, eller på annat sätt bryter mot avtalets krav och förutsättningar, och underlåter att vidta rättelse efter Region Norrbottens påpekanden. Vitet kan maximalt vara två procent av kontraktets totala värde, per vecka, och uppgå till totalt maximalt fyra veckor. Om bristen är av särskild vikt eller det föreligger risk för patienter kan regionen innehålla kvarstående beställningsvolym av kontraktet tills dess att bristen är åtgärdad.

Intervjuer

Under intervjuerna beskrivs att arbetet med avtalen primärt görs av regionjurist. Avtalen är inte granskade av extern rådgivare (“second opinion”) och det beskrivs inte att arbetet sker i en tvärsektoriell arbetsgrupp, processorienterat eller liknande.

Bedömning

Har regionen implementerat de identifierade kraven på ett ändamålsenligt och effektivt sätt i avtalen med de upphandlade leverantörerna? Svar: Delvis

Avtal, vårdval primärvård

Vi noterar en viss sammanblandning av vad vi bedömer vara krav på leverantören, samt förutsättningar för att få ansluta till LOV-systemet, och villkor för själva utförandet (det vill säga avtalsvillkoren). Det gör att det är svårt att få en överblick över vilka delar som avser krav och förutsättningar för ett godkännande, och vad som är villkor som gäller framåtsyftande avseende parternas relation och den levererade tjänsten. Vi noterar även ett antal oklara och eventuellt motsägande krav/villkor mellan dokumenten Beställning Vårdval primärvård 2023 och avtalsmallen för vårdval primärvård. Ett exempel är beskrivningen av sanktioner vid bristande efterlevnad av avtalet.

De allmänna kraven att vårdgivaren ska följa gällande lagar, regler och regionens vid var tid gällande policies bedömer vi vara ett tydligt grundläggande villkor. Dock blandas denna typ av villkor med mer otydliga sådana. Ett exempel är att avseende föreskrift om journalföring och behandling av personuppgifter anges att denna ska “utgöra grunden” för journaldokumentation. Den typen av “dubbelregleringar, där dessutom olika begrepp och kravnivåer används, riskerar att göra avtalet otydligt. Därmed finns en risk för att villkoren kan tolkas på annat sätt än vad som var avsett, och därmed blir regionens styrning och reglering av leverantör och tjänst sämre.

I relation till detta bedömer vi även att regleringen av leverantörens kvalitetsledningssystem och interna kontroll är omotiverat otydlig. Det anges att Socialstyrelsens föreskrift ska tillämpas och att ett "ändamålsenligt" internkontrollsystem ska kunna redogöras för. Ett tydligare villkor, som också hade varit enklare att följa upp hade varit att vårdgivaren årligen ska lämna in sitt ledningssystem avseende informationssäkerhet och dokumenterade uppföljning av detta, för att visa upp efterlevnaden av exempelvis Socialstyrelsens föreskrift om journalföring och behandling av personuppgifter. På det sättet skapas ett tydligt krav som är objektivt förankrat, aktivitetsansvaret (i detta fall att lämna in dokumentationen) ligger på leverantören, och det skapas en transparens som förenklar regionens åtagande i relation till exempelvis kommunallagen.

I avtalet stadgas också att regionen kan säga upp en leverantör i förtid för att denne inte följer de krav som uppställs i regelverket för Vårdval Norrbotten. Den typen av villkor är i grunden bra, men för att det ska vara möjligt att tillämpa på ett effektivt sätt krävs att kraven som det hänvisas till är tydliga. Och det behöver vara tydligt när ett agerande följer reglerna, och när det inte sker. Avseende just detta exempel blir villkoret otydligt eftersom det inte är definierat vad som avses med “regelverk” (det samlade upphandlingsunderlaget, avtalet, interna styrdokument, lagstiftning eller något annat?).

Genomgående i detta avtal beskrivs relativt otydliga krav, och där det även är oklart vem av parterna som har tolkningsföreträde i olika situationer. Ett exempel är skrivningen avseende brandvägg, där leverantören “rekommenderas” att ha en brandvägg av “lämplig” storlek och märke. Med den typen av skrivning kan det i ett senare skede vara mycket svårt att visa på en brist hos leverantören, som kan läggas till grund för exempelvis att säga upp avtalet.

Avseende regionens möjlighet till uppföljning ges vissa möjligheter. De uttrycks dock på ett relativt oklart och oprecist sätt. Beroende på hur vissa skrivningar kan tolkas finns risk för att det inte föreligger någon möjlighet för regionen, utifrån avtalsvillkoren, att kunna utföra fullständiga avtalsrevisioner. Det innebär att det kan vara svårt för regionen att kontrollera om de krav man satt upp följs av leverantören, vilket får anses vara en brist.

Avtal, ramavtal operationstjänster

Villkoret att leverantören ska följa alla tillämpliga lagar, föreskrifter och branschpraxis är i sig ett relativt tydligt villkor. I detta avtal läggs dock flera villkor till, som inte är lika tydliga. Det gör att villkoren sammantaget blir otydliga och öppnar upp för tolkningar. När det gäller specifikt informationssäkerhet bedömer vi det som obalanserat att nämna specifikt autentisering (och utelämna många andra relevanta krav och villkor avseende informationssäkerhet), istället för att förtydliga att exempelvis föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården ska följas. Vi ställer oss också frågande till formuleringen “patientdatalag eller motsvarande”

utifrån att det inte finns någon annan reglering som kan vara alternativ till patientdatalagen.

Även regleringen av sekretess och tystnadsplikt bedömer vi som otydlig. För enskilda vårdgivare och dess anställda (som inte omfattas av OSL) regleras tystnadsplikten i patientsäkerhetslagen. Utöver det finns även andra lagar om tystnadsplikt som kan aktualiseras. Hänvisningen till OSL är därför till viss del missvisande. I villkoret används också begreppet “utomstående” (det vill säga att leverantörens anställda får inte förmedla konfidentiell information till utomstående). Ett lämpligare begrepp är “obehöriga”. Dels för att använda likalydande begrepp som lagstiftningen, men även för att även personer inom en vårdgivares organisation kan vara obehöriga mottagare av viss information.

Ett alternativt villkor, som hade stärkt skyddet för sekretessbelagd information och gjort det lättare för regionen att följa upp efterlevnaden, hade varit att binda leverantören till att dess anställda och uppdragstagare hade behövt underteckna sekretessförbindelse. Denna kan vara utformad av regionen och det kan även villkoras om att den ska lämnas till regionen. Utöver detta hade även en enklare och mer övergripande formulering avseende sekretess och tystnadsplikt varit ett mer effektivt avtalsvillkor.

Avseende uppföljning är det positivt att regionens revisorer ges stor möjlighet till insyn och åtkomst till information. Det hade varit önskvärt att det hade varit tydligare skrivningar kring regionens egna möjligheter till uppföljning, insyn och tillgång till information. Det hade även varit fördelaktigt om det hade tydliggjorts att avtalet kan följas upp på det sätt och vid de tillfällen som regionen beslutar. Med nuvarande villkor och skrivningar lämnas utrymme för invändningar och diskussion, vilket är en onödig begränsning och kan leda till merarbete för regionens del. För att regionen ska kunna leva upp till de lagstadgade kraven i kommunallag och hälso- och sjukvårdslag krävs även en relativt omfattande insyn och kontroll.

De vitesmöjligheter som regionen har är generellt bra, men det krävs stora insatser från regionen för att ett vite överhuvudtaget ska komma till stånd. Man måste först konstatera en brist genom en omfattande uppföljning (utifrån hur krav och avtalsvillkoren är formulerade inom detta område krävs det relativt omfattande uppföljning för att det ska gå att konstatera brister) alternativt utreda en incident. Allt detta behöver regionen själva dokumentera eftersom det är regionen som kommer ha ”bevisbördan” för att påvisa en brist (utifrån hur avtalen är skrivna). Och därefter behöver man administrera processen att kräva in vitet. Detta talar för att det är en relativt hög tröskel för att använda denna sanktion.

I övrigt är även bedömningen att detta avtal i viss utsträckning saknar effektiva sanktionsmöjligheter och incitament för vårdgivarna att följa avtalen, avseende informationssäkerhet. Exempelvis saknas helt målrelaterad ersättning avseende detta område. Vi har heller inte kunnat konstatera några avtalsvillkor som stimulerar utveckling eller proaktivitet avseende informationssäkerhet.

Uppföljning av upphandlingskrav och avtalsvillkor

Revisionsfråga 3: Följer regionen upp att de avtalade kraven och villkoren följs av leverantörerna på ett ändamålsenligt sätt?

Iakttagelser

Styrande dokument

I regionens styrande dokument *Anvisning för avtalsförvaltning* anges att avtalsägaren ska säkerställa att uppföljning av leverans och kvalitet för inköpta tjänster genomförs. Det anges även att avtalsägaren ska utse resurser för avtalsuppföljning. Under intervjuerna framkommer att det är väl känt och etablerat att avtalsägaren har detta ansvaret.

I Anvisning för IT och informationssäkerhet anges att regionen ska engagera sig för efterlevnaden av relevanta lagstiftningar, förordningar och avtalsmässiga skyldigheter. Det förtydligas inte närmare vad det innebär.

Upphandlingsunderlag/Avtal

I avtalet för operationstjänster anges att Region Norrbotten äger rätt att följa upp verksamhet och prestationer samt försäkra sig om att leverantören (och eventuella underleverantörer) uppfyller sina åtaganden enligt avtalet. Det anges även att regionen äger rätt att genomföra fördjupade uppföljningar av leverantörens utförande av uppdraget. Det anges även att avtalet ska följas upp vid behov. I upphandlingsunderlaget för LOV-upphandlingen anges att en uppföljningsplan avseende den upphandlade verksamheten fastställs årligen samt att mål och indikatorer används som underlag i uppföljningen.

Intervjuer

Av både granskade dokument och intervjuer framgår att det finns etablerade strukturer och arbetssätt för att följa upp leverantörernas verksamheter, där informationssäkerhet hade kunnat inkluderas. Exempelvis finns rutin avseende att genomföra stickprovskontroll på avtal. Det framkommer dock i granskningen att uppföljning av kraven och villkoren avseende informationssäkerhet ej genomförs. Området finns heller inte med i beslutad uppföljningsplan avseende LOV primärvård. Däremot genomförs uppföljning av avtalen utifrån andra perspektiv.

Bedömning

Följer regionen upp att de avtalade kraven och villkoren följs av leverantörerna på ett ändamålsenligt sätt? Svar: Nej

Utifrån det material och den information vi fått till oss under granskningen kan vi inte se att uppföljning av kraven och villkoren avseende leverantörernas informationssäkerhet genomförs.

Bristen på kontroll gör också att vi bedömer att regionstyrelsen inte följer upp sina leverantörsrelationer på sådant sätt som både interna styrdokument och lagstiftning kräver. Detta innebär i sin tur att det kan föreligga risk för både patienternas säkerhet, deras integritet och för verksamhetens förmåga till kontinuitet. Dessa risker kan i sin tur innebära risk för ekonomiska skador för regionen, exempelvis i form av krav från enskilda som lidit risk på grund av regionens agerande, eller på grund av att krisåtgärder behöver sättas in om privata vårdgivare drabbas av produktionsbortfall.

Exempel på uppföljning och avtalsrevision som kan göras, och till viss del krävs utifrån lagkrav och praxis är;

- Kontroll på plats hos vårdgivaren avseende exempelvis den fysiska IT-miljön, att regler kring säkerhetskopiering följs eller hur kasserad hårdvara hanteras,
- Redogörelse med tillhörande dokumentation från vårdgivaren som visar hur exempelvis socialstyrelsens föreskrift om journalföring och behandling av personuppgifter följs,
- Simulation av incidenter, penetrationstest eller liknande för att testa hur leverantörens skydd och arbetssätt fungerar i praktiken.

Revisionsfråga 4: I det fall avvikelser upptäcks, har regionen ett ändamålsenligt sätt att hantera dessa avvikelser?

Iakttagelser

Styrande dokument

I *Anvisning för IT och informationssäkerhet* beskrivs övergripande hur regionen ska arbeta med leverantörer, avseende informationssäkerhet. Det beskrivs även övergripande hur incidenter ska hanteras i regionen. Det beskrivs dock inte hur avvikelser avseende informationssäkerhet hos leverantörer, antingen genom incidenter eller genom bristande avtalsefterlevnad, ska hanteras.

Anvisning för hantering av informationssäkerhetsavvikelser styr hur avvikelser avseende informationssäkerhet ska hanteras. I den framgår att en avvikelse kan identifieras genom en leverantörsgranskning, samt att en avvikelse ska utredas, dokumenteras, korrigeras och att eventuella konsekvenser ska hanteras. Det framgår dock inte mer konkret hur detta ska gå till eller närmare om roller och ansvar. Det beskrivs inte heller hur ovan beskrivna moment ska hanteras i det fall de sker hos en leverantör.

Avseende LOV inom primärvården har vi inte kunnat identifiera någon beskriven handlingsplan, rutin eller liknande som beskriver hur en avvikelse avseende informationssäkerhet ska hanteras.

Avseende leverantörer upphandlade genom upphandlingsenheten (i detta fall LOU-avtalet) finns rutinen *Problem med leverantörer*. I denna framgår att det är upphandlaren som ansvarar för hanteringen av problem som är så pass betydande att det handlar om bristande avtalsefterlevnad, eller avvikelser från överenskomna villkor.

Av rutinen framgår vidare att upphandlaren kan behöva kräva in vite, häva avtalet m.m. Dock framgår inte mer konkret hur ett sådant arbete ska initieras eller praktiskt gå till väga.

Avtal

I LOV-avtalet framgår att om leverantören brister i sin uppfyllelse av avtalet så har regionen rätt att fatta beslut om vite intill dess att bristen är åtgärdad. I avtalet finns ingen fastställd nivå eller modell för vitet, utan det framgår endast att vitet ska vara skäligt i förhållande till felet och inte får överskrida 100 procent av maximal månadsersättning.

Det framgår även att regionen har rätt att i förtid säga upp avtalet (med den uppsägningstid som regionen bestämmer) om leverantören visar sig till väsentlig del inte uppfylla de krav som uppställs i regelverket för Vårdval Norrbotten. Detta kan exempelvis inträffa om leverantören agerar på sådant sätt att det allvarligt skadat förtroendet för regionen som beställaren och inte vidtar rättelse inom skälig tid efter skriftligt påpekande från regionen.

I LOU-avtalet anges att alla avvikelser av betydelse för att undvika skador och störningar ska registreras i ändamålsenligt system enligt gällande föreskrifter. Dock tydliggörs inte vidare vilken typ av avvikelser som avses, eller vilka system eller föreskrifter som åsyftas.

Det framgår också att regionen har möjlighet att utfärda vite eller sanktioner om leverantören inte uppfyller åtaganden enligt avtalet eller dess bilagor, eller på annat sätt bryter mot avtalets krav och förutsättningar, och underlåter att vidta rättelse efter Region Norrbottens påpekanden. Vitet kan maximalt vara två procent av kontraktets totala värde, per vecka, och uppgå till totalt maximalt fyra veckor. Om bristen är av särskild vikt eller det föreligger risk för patienter kan regionen innehålla kvarstående beställningsvolym av kontraktet tills dess att bristen är åtgärdad.

Vidare framgår att regionen har möjlighet att säga upp avtalet om leverantören väsentligt avseende åsidosätter sina förpliktelser enligt avtalet och inte inom rimlig tid, trots skriftligt påpekande, vidtar rättelse. Regionen har även rätt att med omedelbar verkan häva avtalet vid upprepade brister i utförandet eller vid grov vårdslöshet. Bristande efterlevnad av gällande lagar och förordningar räknas som grov vårdslöshet enligt avtalsvillkoret.

Intervjuer

Under intervjuer framgår att avvikelser avseende informationssäkerhet ej har identifierats hos de privata vårdgivarna. Det har heller inte kunnat redogöras för en konkret hantering av detta i det fall det skulle ske. Utifrån intervjuerna framstår det även som något oklart vems ansvar inom regionen att hantera avvikelser avseende informationssäkerhet hos privata vårdgivare, och i vilken process en sådan avvikelse hanteras.

Bedömning

I det fall avvikelser upptäcks, har regionen ett ändamålsenligt sätt att hantera dessa avvikelser? Svar: Delvis

De formella förutsättningarna för en effektiv uppföljning, och efterföljande åtgärder, ges i upphandlingsunderlagen och avtalen. För att det ska finnas möjligheter till effektiv och incitamentsskapande uppföljning behöver avtalen vara konstruerade på ett flexibelt sätt, där regionen ges stort utrymme till egna bedömningar. Dessa bedömningar kan självklart alltid prövas rättsligt, men det är viktigt att den initiala valmöjligheten ligger hos regionen, och att man inte är beroende av någon form av bekräftelse eller liknande från vårdgivarens sida.

Balansgången när dessa villkor konstrueras är mellan regionens intresse, och att det fortfarande måste vara affärsmässigt motiverat för en vårdgivare att vilja ingå avtal med regionen. Ytterligare en faktor i sammanhanget är att en riskbedömning behöver göras; möjligheterna till påföljder behöver stå i relation till de risker som uppstår vid olika typer av brister.

Exempel på sanktioner/påföljder som normalt sett är effektiva, är innehållande av betalning. Den typen av villkor skapar starka incitament att följa avtalet, och det är också administrativt mindre arbetskrävande än viten eftersom det innebär färre transaktioner. Ett annat exempel är en avstängningsmöjlighet till tjänster och system som vårdgivaren är beroende av för att kunna utföra sin verksamhet.

Utifrån de granskade styrande dokumenten bedömer vi att det är otydligt både för anställda hos regionen, men även för leverantörerna hur man ska gå tillväga i det fall en avvikelse upptäcks. Vi bedömer att detta bekräftas under intervjuerna utifrån att vi inte kunnat få tydliga redogörelser för hur en avvikelse avseende informationssäkerhet skulle hanteras.

Avtalen ger viss vägledning till vilka konsekvenser avvikelser kan få. Vår bedömning är dock att sanktionsmodellerna, avseende båda avtalen, är relativt outvecklade. Det är en brist i LOV-avtalet att vitesnivåerna inte är fastställda. I LOU-avtalet är situationen något bättre utifrån att vitesnivån är fastställd. Dock framstår nivån som låg i relation till riskerna (exempelvis har ett avtal som har ett maximalt värde på en miljon, ett vitestak på 80 000 kr) som bristande informationssäkerhet kan innebära. I LOV-avtalet framgår att regionens anspråk avseende vite kan kvittas mot leverantörens anspråk på ersättning. Motsvarande villkor kan vi inte återfinna i LOU-avtalet. Villkoret är ett exempel på ett effektivt villkor utifrån att det skapar ett starkare incitament gentemot leverantören, och är administrativt enkelt att hantera.

Sammantaget görs bedömningen att utifrån styrande dokument och avtalsvillkor har regionen inte skapat ändamålsenliga formella förutsättningar för att kunna hantera avvikelser. Vi kan heller inte se att det finns ett etablerat arbetssätt i praktiken för att hantera avvikelser hos privata vårdgivare avseende informationssäkerhet.

Samlad bedömning

PwC har på uppdrag av de förtroendevalda revisorerna i Region Norrbotten genomfört en granskning av avtalsstyrning och uppföljning av privata vårdgivares informationssäkerhet. Granskningen syftar till att bedöma om regionstyrelsen säkerställer en ändamålsenlig avtalsstyrning och uppföljning av privata vårdgivares informationssäkerhet samt ifall den interna kontrollen i sammanhanget är tillräcklig. Granskningen syftar även till att säkerställa att regionen uppfyller kommunallagens krav om internkontroll.

Utifrån digitalisering och omvärldsutvecklingen är informationssäkerhet idag en avgörande faktor, avseende både säkerhet, förtroende och förmåga till kontinuitet. Det innebär att en vårdgivare måste försäkra sig om att följa lagar och regler inom området, och arbeta aktivt med utveckling och uppdatering för att hela tiden vara a jour med omvärldsutveckling och förväntan från bland annat patienter. För regionens egen verksamhet sker detta inom den egna organisationen och inom ramen för den interna styrningen. Men när verksamheten ligger hos en extern part behöver styrningen av detta ske i kravställningen (inklusive kvalificering och utvärdering) och i avtalsvillkoren.

Utifrån detta perspektiv gör vi bedömningen att kravställning, val av kriterier i kvalificering och utvärdering samt avtalsvillkor i större utsträckning behöver präglas av en riskbedömning avseende vilka specifika risker som behöver hanteras inom olika typer av upphandlingar. Vi bedömer också att avtalsvillkoren behöver kompletteras med incitament för vårdgivare att i större utsträckning arbeta med informationssäkerhet som en del av deras förmåga till säker drift, kontinuitet och kvalitetsutveckling. Kunskap och medvetenhet kring vilka risker som kan kopplas till informationshantering av olika slag har ökat drastiskt de senaste åren, och detta bedömer vi bör avspeglas tydligare i regionstyrelsens upphandlingar av vård.

Bristen på kontroll och strukturerad avvikelsehantering inom detta område, innebär också att vi bedömer att det finns en risk för att regionen inte har kontroll på vilken förmåga till kontinuitet, och vilken säkerhets-/risknivå verksamheten har som helhet (det vill säga både den egna driften samt vården som utförs av privata vårdgivare). Exempelvis innebär den låga graden av uppföljning och kontroll att det kan vara svårt att bedöma sårbarheter och därmed kunna prioritera insatser. Eller bedöma om krav eller avtalsvillkor behöver förändras utifrån nuvarande status avseende vårdgivarnas arbete på detta område.

Utifrån ett affärsmässigt perspektiv bedömer vi det inte heller som helt ändamålsenligt med så liten grad av uppföljning, avseende ett område som är så viktigt för regionstyrelsens förmåga att uppfylla sitt lagstadgade uppdrag. Brister inom detta område kan betyda avsevärda förtroendeskador och kostnadsökningar för regionstyrelsen, och därför bör detta område ses som en kritisk del av tjänsten man upphandlar. Det innebär i sin tur att uppföljningen behöver prioriteras på samma nivå som exempelvis den ekonomiska uppföljningen.

Under granskningen noterar vi dock att lyhördheten och intresset för den problematik vi beskriver kopplat till privata vårdgivare och informationssäkerhet, är påtaglig. Vi förstår också att det skett ett utvecklingsarbete i frågorna de senaste åren, som åtminstone skapat större grad av medvetenhet. Ett led i utvecklingsarbetet handlar om att omhänderta och åtgärda de rekommendationer som gavs i en tidigare revisionsgranskning, *Granskning av informations- och cybersäkerhet*, från juni 2022. Vi har också uppfattat att resurserna som avsätts till informationssäkerhetsarbete planeras att öka. Sammantaget innebär det att vi noterar att det finns en positiv trend, att viss medvetenhet om problematiken finns, och även en ambition att hantera den.

Utifrån genomförd granskning är vår samlade bedömning att regionstyrelsen i Region Norrbotten **inte helt** säkerställer en ändamålsenlig avtalsstyrning och uppföljning av privata vårdgivares informationssäkerhet. Vi bedömer **ej** att den interna kontrollen är tillräcklig.

Sammanfattande bedömningar utifrån revisionsfrågor

Revisionsfråga	Bedömning	
1. Har regionen säkerställt att tillräckliga krav ställs på privata vårdgivare i samband med upphandling utifrån ett legalt, säkerhetsmässigt och affärsmässigt perspektiv?	**Delvis** Krav avseende informationssäkerhet har direkt eller indirekt inkluderats i båda upphandlingsunderlagen. Kraven bedöms dock inte vara tillräckliga.	
2. Har regionen implementerat de identifierade kraven på ett ändamålsenligt och effektivt sätt i avtalen med de upphandlade leverantörerna?	**Delvis** Krav och villkor avseende informationssäkerhet är till viss del implementerade i avtalen. Dock inte på ett helt ändamålsenligt eller tillräckligt sätt.	
3. Följer regionen upp att de avtalade kraven och villkoren följs av leverantörerna på ett ändamålsenligt sätt?	**Nej** Utifrån det material och den information vi fått till oss under granskningen kan vi inte se att uppföljning av kraven och villkoren avseende leverantörernas informationssäkerhet genomförs.	
4. I det fall avvikelser upptäcks, har regionen ett ändamålsenligt sätt att hantera dessa avvikelser?	**Delvis** Formella förutsättningar för att genomföra uppföljning och hantera efterföljande avvikelser har etablerats. Förutsättningarna bedöms dock inte vara helt ändamålsenliga. Etablerade arbetssätt för att i praktiken hantera avvikelser avseende informationssäkerhet har inte heller identifierats.	

Kristian Damlin

Uppdragsledare

Charlotte Arnell

Projektledare