REGIONREVISORERNA

RAPPORT NR 9/2022

Externa vårdgivares informationssäkerhet

Region Stockholm

Kort om rapporten

Hälso- och sjukvårdsnämnden upphandlar vård från drygt 2 000 externa vårdgivare. Det innebär att en betydande del av sjukvården bedrivs utanför regionens organisation. Nämndens krav gällande informationssäkerhet regleras därför i upphandlingen och i avtalsvillkor. Den systematiska uppföljningen av att villkoren följs bör stärkas så att nämnden får vetskap om hur väl respektive vårdgivare följer avtalskraven. Dessutom har nämnden då möjlighet att som helhet bedöma eventuella sårbarheter och därmed kunna prioritera insatser.

Regionrevisorerna

2023-02-22

Diarienummer
RK 2019-0044

Hälso-och sjukvårdsnämnden

Projektrapport 9/2022
Externa vårdgivares informationssäkerhet

Revisorerna i revisorsgrupp II beslutade vid sitt möte den 2023-02-22 överlämna rapporten till hälso- och sjukvårdsnämnden för yttrande senast 2023-05-31.

Revisorernas samlade bedömning är att HSN:s arbete med framtagande av kravspecifikationer och avtalsvillkor avseende informationssäkerhet har stärkts de senaste åren. Däremot visar granskningen att det i praktiken inte sker någon systematisk uppföljning av externa vårdgivarens informationssäkerhet. Det innebär att nämnden inte har någon kunskap om avtalskraven inom informationssäkerhetsområdet följs.

Revisorerna vill särskilt ha svar på hur hälso- och sjukvårdsnämnden avser att

- säkerställa en återkommande systematisk uppföljning av externa vårdgivares informationssäkerhet.

I övrigt hänvisar revisorerna till revisionskontorets kappa med bifogad konsultrapport.

Paragrafen förklarades omedelbart justerad.

Hans-Erik Salomonsson
ordförande

Karelia Pagan
sekreterare

Region Stockholm
Regionrevisorerna
Box 22230
104 22 Stockholm

Telefon: 08-737 25 00
E-post:
regionrevisorerna.rev@regionstockholm.se

Säte: Stockholm
Org.nr: 232100-0016
www.regionstockholm.se

Besök oss: Hantverkargatan 25B, T-bana Rådhuset, se www.sl.se

1 Slutsatser och rekommendationer

Hälso- och sjukvårdsnämnden upphandlar vård från drygt 2 000 externa vårdgivare. Det innebär att en betydande del av sjukvården i regionen bedrivs av externa vårdgivare utanför regionens organisation, som inte omfattas av regionens styrsystem när det gäller informationssäkerhet. Eftersom dessa vårdgivare använder vissa av regionens system och är uppkopplade på regionens nät riskerar brister i externa vårdgivares informationssäkerhetsarbete orsaka skada som kan påverka tillgången till viktig information för hälso- och sjukvården. Revisionen har därför granskat om hälso- och sjukvårdsnämnden säkerställer en systematisk avtalsstyrning och uppföljning av externa vårdgivares informationssäkerhet.

Granskningen har, under ledning av revisionskontoret i Region Stockholm, genomförts av upphandlad konsult. Revisionen har nedan sammanfattat de slutsatser som kan dras och lämnar rekommendationer med anledning av granskningen. Ansvarig projektledare vid revisionskontoret har varit Max Eliasson. Konsultens iakttagelser och bedömningar i sin helhet framgår i bilaga. Ansvarig konsult har varit Charlotte Arnell vid PwC.

1.1 Kravställning

Det finns en dokumenterad process för kravställning av bland annat informationssäkerhet vid upphandling av externa vårdgivare. I alla underlag ställs kravet att vårdgivarna ska följa lagar, förordningar och föreskrifter, de vid var tid gällande policys och riktlinjer avseende informationssäkerhet som beslutas om av Region Stockholm, att informationsskyddet ska dokumenteras samt att den informationen ska kunna delges Region Stockholm på begäran. I övrigt skiljer sig detaljeringsgraden åt mellan avtalsområden och hur gamla avtalet är.

Revisionen bedömer att nämndens arbete med framtagande av kravspecifikationer och avtalsvillkor avseende informationssäkerhet har stärkts de senaste åren. I de äldre avtalen skulle det mer tydligt kunna framgå vilka interna styrdokument som är obligatoriska och i vilken utsträckning som informationen på vårdgivarguiden.se ska ses som bindande eller endast är vägledande. De olika vårdområdena som upphandlas kan ha olika typer av risker som behöver beaktas och dokumenteras. Revisionen bedömer därför att kravställning, val av kriterier i kvalificering och utvärdering samt avtalsvillkor i större utsträckning bör präglas av en riskbedömning avseende vilka specifika informationssäkerhetsrisker som behöver hanteras inom olika typer av upphandlingar. Avtalen bör i sin tur mer tydligt specificera vilka informationssäkerhetskrav som ställs på vårdgivaren. Aktuella vårdgivare behöver också i större utsträckning verifiera sitt informationssäkerhetsarbete redan vid upphandling och innan avtalstecknande.

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. Revisionen menar därför att avtalsvillkoren bör kompletteras med incitament för vårdgivare att i större utsträckning arbeta med informationssäkerhet som en del av deras förmåga till säker drift, kontinuitet och kvalitetsutveckling.

1.2 Uppföljning

Revisionen har tidigare rekommenderat hälso- och sjukvårdsnämnden att skapa rutiner för uppföljning av informationssäkerhet gentemot externa vårdgivare.[1] Den nu genomförda granskningen visar att nämndens struktur för uppföljning av informationssäkerhet hos de externa vårdgivarna har utvecklats de senaste åren. Modellen innebär att uppföljning ska ske via en översiktlig enkät som planeras att implementeras från 2023.

Granskningen visar att det i praktiken inte sker någon systematisk uppföljning av externa vårdgivarens informationssäkerhet. Det innebär att nämnden inte har någon kunskap om avtalskraven inom området följs. Uppföljning av informationssäkerhet är heller inte ett riskområde som ingår i nämndens internkontrollplan 2022. En viss uppföljning/kontroll sker om vårdgivarna ska anslutas till olika typer av tjänster eller SLLnet[2]. Även när den nya uppföljningsmodellen har implementerats behöver denna årliga uppföljning kompletteras med en mer detaljerad uppföljning av upphandlade vårdgivare.

Avsaknaden av en systematiskt och dokumenterad uppföljning innebär också att det finns risk för att det saknas kunskap om regionens förmåga till kontinuitet, som helhet (det vill säga både den egna driften, egna bolagen samt vården som utförs av externa vårdgivare). Exempelvis innebär den låga graden av reell kontroll att det kan vara svårt att bedöma sårbarheter och därmed kunna prioritera insatser. Det är också svårt att bedöma om krav eller avtalsvillkor behöver förändras utifrån nuvarande status avseende vårdgivarnas arbete med informationssäkerhet. Brister inom detta område kan betyda avsevärda förtroendeskador och kostnadsökningar för hälso- och sjukvårdsnämnden och därför bör detta område ses som en kritisk del av tjänsten som upphandlas.

Revisionen bedömer att det fortfarande återstår utvecklingsområden för att nämnden ska uppfylla kommunallagens krav om intern kontroll och fullmäktiges styrande dokument för informationssäkerhet[3] när det gäller en systematisk uppföljning av leverantörer. Det är positivt att arbetet med metoder för uppföljning av informationssäkerhet hos de externa vårdgivarna har intensifierats och utvecklats. Men revisionen bedömer det också som rimligt att det får ännu högre prioritet, och sker med en högre grad av angelägenhet, utifrån de risker som finns på området. Tidigare lämnad rekommendation till nämnden kvarstår därmed i avvaktan på att den nya modellen implementerats.

1.3 Rekommendationer

- Hälso- och sjukvårdsnämnden bör säkerställa en återkommande systematisk uppföljning av externa vårdgivares informationssäkerhet.
- Ledningen bör inkludera uppföljning gällande informationssäkerhet i den interna kontrollplanen.
- Ledningen 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 inom olika typer av upphandlingar.

[1] Årsrapport 2018 Hälso- och sjukvårdsnämnden
[2] Fjärrnätet för datakommunikation mellan verksamheter i region Stockholm
[3] Policy för verksamhetsskydd (RS 2020-0147), Riktlinjer för informationssäkerhet (RS 2020-0148)

Bilaga 1 Konsultens rapport - Styrning och uppföljning av informationssäkerhet vid upphandling av externa vårdgivare

Styrning och uppföljning av informationssäkerhet vid upphandling av externa vårdgivare

Region Stockholm

Januari 2023

Rebecka Hansson

Charlotte Arnell

Simon Granberg

pwc

Granskningspromemoria

Innehållsförteckning

Förkortningar och begrepp

GDPR	Den allmänna dataskyddsförordningen
HSN	Hälso- och sjukvårdsnämnden i Region Stockholm
HSF	Hälso- och sjukvårdsförvaltningen i Region Stockholm
HSL	Hälso- och sjukvårdslag
IVO	Inspektionen för vård och omsorg
LOU	Lag om offentlig upphandling
LOV	Lag om valfrihetssystem
SLLNET	Region Stockholms kommunikationsnätverk
VBU	Vårdbeställarutskottet i HSN
Vårdgivarguiden.se	Hemsida med information material och tjänster för alla vårdgivare inom Region Stockholm

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. Brister i hantering av information vid detta uppdrag kan bland annat leda till skador i verksamheterna, skador för enskilda och ett försämrat förtroende för tjänster och bakomliggande aktörer.

Hälso- och sjukvårdsnämnden (HSN) i Region Stockholm upphandlar vård från drygt 2 000 externa vårdgivare. Det innebär att en betydande del av sjukvården i regionen bedrivs utanför regionens organisation. Vilket i sin tur innebär att den enda egentliga styrningen av denna verksamhet som regionen kan utföra, är genom att ställa rätt krav vid upphandling, säkerställa att dessa krav, tillsammans med ändamålsenliga villkor, avtalas om med vinnande och godkända leverantörer, därefter följa upp att avtalen följs, samt vid avvikelser vidta ändamålsenliga åtgärder.

Enligt Region Stockholms riktlinjer[1] ska informationssäkerhet och skyddskrav vara en naturlig del av en upphandling. Regionens revisorer har identifierat en risk för att HSN inte ställer tydliga krav på informationssäkerhet i de avtal som tecknas med externa vårdgivare och att HSN inte i tillräcklig omfattning följer upp de krav som ställs.

[1] RS xxxx-xxx

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 Stockholm inte har ett eget, självständigt ansvar för att en kontrakterad 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.

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 som inte finns till hands när den behövs kan innebära stora negativa konsekvenser för både en verksamhet och enskilda individer. Informationssäkerhet handlar om att 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 största 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 Stockholm 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 i en registrerad databas, 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 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 Stockholm bedriver vård både i egen regi, genom egna bolag och genom att upphandla externa vårdgivare enligt både LOU och enligt LOV.

Syfte och revisionsfrågor

Granskningen syftar till att bedöma om hälso-och sjukvårdsnämnden säkerställer en ändamålsenlig avtalsstyrning och uppföljning av externa vårdgivares informationssäkerhet.

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

1. **Har HSN identifierat vilka krav som behöver ställas på externa 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.

2. **Har HSN en ändamålsenlig metod för att de identifierade kraven i punkt 1 säkerställs genom hela upphandlingsprocessen?**

   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.

   Ett annat viktigt syfte med ett systematiskt arbetssätt handlar om det organisatoriska lärandet, nämligen att de erfarenheter och läranden som hela tiden sker, fångas upp och tas med i nästa upphandling. Detta är viktigt för att uppnå ett kontinuerligt utvecklingsarbete och där förbättringar hela tiden genomförs.

3. **Har HSN 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

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

   Både upphandlingskrav och avtalsvillkor är teoretiska faktorer. 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 bland annat vara lämpligt att följa upp genom exempelvis simulerade incidenter, tester av olika slag, samt kontroll att leverantören har olika typer av dokumentation på plats.

5. **I det fall avvikelser upptäcks, har HSN 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.

Utöver ovan angivna beskrivna granskning har det även ingått i PwC:s uppdrag att följa upp den granskning av informationssäkerhet hos externa vårdgivare som regionrevisionen genomförde 2018.

Bedömningsgrunder

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 externa 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 att regionens kapacitet och förmåga att leva upp till lagstiftningens krav inte försämras.

Socialstyrelsens föreskrifter och allmänna råd om ledningssystem för systematiskt kvalitetsarbete, SOSFS 2011:9
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, HSLF-FS 2016:40
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 externa vårdgivare, där avtalen är gällande vid tidpunkten för granskningen. Eftersom fokuset för denna granskning har varit leverantörsstyrning och -uppföljning, har endast vårdgivare som upphandlats på öppna marknaden inkluderats. Det innebär att den verksamhet som bedrivs i egen drift och genom regionens egna bolag inte är inkluderad i denna granskning. Inte heller ingår vårdgivare verksamma enligt lag om läkarvårdsersättning eller lag om ersättning för fysioterapi, som är verksamma i Region Stockholm då HSN inte reglerar dessa verksamheter.

Metod
Granskningen har genomförts genom att regionens styrande och stödjande (exempelvis mallar och instruktioner) dokument granskas. Utdrag ur Avtalshandboken har erhållits och hemsidan vårdgivarguiden.se har studerats. Även andra dokument har granskats såsom beslutsunderlag och granskningsrapporter. Därefter har intervjuer hållits med några berörda befattningar.

De intervjuade har beretts möjlighet att sakgranska rapporten.

Utöver ovan har även granskning av upphandlings-/LOV-underlag med tillhörande avtal genomförts. De upphandlingar som valts ut för granskning är

- Upphandling närakut innerstaden
- Vårdval barn- och ungdomsmedicinsk öppenvård
- Vårdval specialiserad hudsjukvård (två upphandlingsunderlag/avtal, dels från 2019, dels från 2022)

Ovan områden har valts ut för att spegla olika typer av vårdområden, de vänder sig både till större och mindre vårdgivare, samt att upphandlingarna är genomförda i relativ närtid för att spegla de aktuella arbetsmetoderna. Eftersom upphandlingsunderlag och avtal ser likadana ut för alla vårdgivare för respektive område, har inga särskilda vårdgivares avtal granskats.

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.

Tidigare granskningar och rekommendationer

Tidigare granskning av Regionrevisionen
2018 granskade revisionen hur HSN hanterade informationssäkerheten hos externa vårdgivare. Revisionen gjorde då bedömningen att krav gällande informationssäkerhet och personuppgifter var tydligt formulerade i avtal med externa vårdgivare. Däremot bedömde man att HSN inte genomförde någon systematiserad och dokumenterad uppföljning för att säkerställa att kraven efterlevs.

Revisionen rekommenderade HSN att snarast skapa rutiner för uppföljning av informationssäkerhet gentemot externa vårdgivare.

Extern granskning med anledning av 1177-incidenten

I början av 2019 blev det känt att inspelningar från vissa samtal till 1177 Vårdguiden på telefon blivit tillgängliga över internet för obehöriga. Incidenten berodde på en felkonfigurerad lagringsenhet hos bolaget Medicall, en underleverantör till vårdgivaren MedHelp AB som i sin tur hade avtal med Region Stockholm om att utföra tjänsten 1177 Vårdguiden.

Med anledning av den allvarliga incidenten genomförde HSN en extern granskning av informationssäkerheten hos 1177 Vårdguiden, samt om kraven i avtalet med Medhelp AB och uppföljningen av avtalet varit ändamålsenliga. Den externa granskningen syftade även till att lämna rekommendationer till förbättringar, för att minimera risken att motsvarande situation skulle kunna uppstå igen.

Bedömningen som gjordes i den externa granskningen var att HSN behövde utveckla kravställningen avseende informationssäkerhet vid upphandling, samt att uppföljningen av icke funktionella krav, bland annat informationssäkerhet, behövde struktureras och formaliseras. Man bedömde att de icke funktionella kraven utgick ifrån ett generellt perspektiv för att passa alla vårdgivare, och inte i tillräcklig utsträckning var anpassade till den specifika vårdsituationen och de risker som följer. När det gäller uppföljningen gjordes bedömningen att de icke funktionella kraven inte följdes upp i proportion till deras betydelse, och den var inte heller heltäckande eller strukturerad avseende hur vårdgivaren hanterade information (exempelvis utifrån perspektivet säkerhet).

Granskningsresultat

Kravställning vid upphandling

Nuvarande arbetssätt avseende upphandlingsprocessen, fram till avtalsuppföljning

Processen för att upphandla externa vårdgivare finns beskriven i Avtalshandboken, som finns på regionens intranät. Handboken infördes 2018 och genomgick en omfattande revidering under hösten 2022.

Processen inleds med en så kallad strategisk analys där det ingår att göra en analys av vårdbehovet, en marknadsanalys och en analys av rådande struktur (exempelvis rättslig reglering, interna styrande dokument, omvärldsanalys och erfarenhetsinhämtning från nuvarande avtal). Arbetet leds och organiseras av HSF:s ledning och bereds bland annat i styrgrupperna för avtalsprojekt som finns på de två beställaravdelningarna. Analysen kan resultera i antingen beslut att inleda upphandling, eller att avsluta avtalsområdet och därmed inte inleda upphandling. Avser beslutet upphandling enligt LOV är beslutet delegerat till avtalsutskottet, och gäller det upphandlingen enligt LOU ska beslutet tas av HSN (om inte värdet understiger 50 miljoner kr, då delegeras beslutet till hälso- och sjukvårdsdirektör).

Om det beslutas att inleda ny upphandling eller ändra ett vårdval, startas nästa steg i processen; att skapa ett avtalsområdesprojekt. Konkret innebär det att upphandlingsunderlaget skapas under denna fas. Enhetschef för den ansvariga

upphandlande enheten formulerar projektdirektiv, tillsätter projektledare, identifierar vilka kompetenser som behövs i projektgruppen och tillsätter projektgrupp i samråd med projektledare. Enligt Avtalshandboken ska juridisk kompetens, vid behov, avropas av enhetschef. Handlar det om en LOU-upphandling ska även upphandlare avropas.

Inom ramen för denna fas ska det interna nätverket som kallas Noden involveras. Nätverket, och ibland med hjälp av särskilt tillsatt expertgrupp, ska säkerställa att den tänkta avtalsstrukturen kan godkännas och är möjlig att hantera utifrån regionens IT-miljö, standarder och strukturer.

Projektplanen, som är det första underlaget som skapas i denna fas, ska godkännas av projektägare (enhetschef för upphandlande enhet), men i de fallen avsteg från standard behöver göras, problem uppkommer, eller andra avvikelser sker, finns olika möjligheter till eskalering. Vissa frågor av särskild vikt, exempelvis strategiska frågeställningar, kan eskaleras till VBU.

När projektplanen är godkänd följer en process av intern och extern dialog och samverkan för att fånga erfarenheter kunskaper och förutsättningar, i syfte att upphandlingen ska möta det behov som finns. Moment som kan ingå i denna fas är exempelvis omvärldsbevakning, intressentanalys, arbete med interna referens- och expertgrupper (exempelvis informationssäkerhet) och leverantörsdialog.

Nästa steg är att skapa en uppdragsbeskrivning för upphandlingen, och i detta steg tas kravspecifikationen för upphandlingen fram. Olika typer av krav tas upp i Avtalshandboken, exempelvis digitala förmågor, lokaler och rapporteringskrav.

I detta skede skapas också uppföljningsplan och -villkor för kommande avtal. Uppföljningsplanen (det vill säga den planerade uppföljningen) utgår i från regionens prioriteringsmodell för avtalsuppföljning, där olika avtal grupperas efter risk- och komplexitetsnivå. Grupptillhörigheten bestämmer i sin tur omfattning och inriktning på uppföljningen.

Efter detta ska avtalsdokument, ersättningsvillkor med mera skapas. Detta görs utifrån malldokument med kommentarer och instruktioner som kan anpassas för respektive upphandling. Slutligen beskrivs även i Avtalshandboken hur förankring och fastställande av upphandlingsunderlaget görs. Processen skiljer sig beroende på upphandling, men exempelvis beskrivs olika typer av förankringsprocesser, hur man avgör vem som är behörig beslutsfattare och hur ärendeprocessen inför ett politiskt beslut går till.

När upphandlingsunderlaget är beslutat annonseras upphandlingsunderlaget. Beroende på om upphandlingen avser LOV eller LOU skiljer sig den fortsatta processen. En LOV-upphandling innebär att vårdgivare får ansöka om att bli ansluta till det aktuella valfrihetssystemet, utifrån de förutsättningar och villkor som annonserats. Ansökningarna prövas gentemot de krav som angivits i underlaget, och processen kommer att fortgå på det sättet så länge valfrihetssystemet består och upphandlingsunderlaget gäller. I Avtalshandboken finns beskrivet hur ansökningar ska bedömas generellt och hur beslutsprocessen ska gå till.

En LOU-upphandling innebär att anbud för att få det annonserade kontraktet ska vara inne före ett visst datum. Därefter görs en kvalificering (det vill säga en prövning av vilka

anbud som uppfyller kraven att bli utvärderade och poängsatta) och utvärdering utifrån de premisser som beskrivits i upphandlingsunderlaget, och beslut tas därefter om vinnande anbud. Precis som för LOV-upphandlingar beskrivs det i Avtalshandboken hur detta ska gå till, och stöd för hur de olika momenten ska utföras ges.

När beslut om godkännande av LOV-ansökningar och tilldelningsbeslut enligt LOU är fattade (och vunnit laga kraft) behöver driftstart planeras. Det görs genom en mängd olika kontroller och informationsinhämtningar, primärt för att den nya vårdgivaren ska kunna ansluta till relevanta system och anslutningar. och för att informationsutbytet ska kunna fungera som planerat.

För den här processen finns ett antal olika checklistor och kontroller som avtalsansvariga på regionen ska göra tillsammans med vårdgivarna. I det fall det uppstår problem med exempelvis en anslutning beskrivs i Avtalshandboken ett antal olika typer av åtgärder som kan vidtas för att lösa problemen. I det fall en driftstart inte kan ske inom sex månader från planerad start anger Avtalshandboken att ett LOV-avtal ska sägas upp, och för ett LOU-avtal ska det undersökas om avtalsbrott föreligger.

Revisionsfråga 1: Har HSN identifierat vilka krav som behöver ställas på externa vårdgivare i samband med upphandling, utifrån ett legalt, säkerhetsmässigt och affärsmässigt perspektiv?

Iakttagelser; Styrande dokument

Region Stockholms riktlinjer för informationssäkerhet utgår från internationell standard avseende styrning och implementering av informationssäkerhet (ISO 27000-serien). Strukturen för styrdokumenten består av Region Stockholms policy för verksamhetsskydd, Region Stockholms riktlinjer för informationssäkerhet, eventuella kompletterande lokala riktlinjer och anvisningar för Informationssäkerhet.

Verksamhetsskyddspolicyn konkretiseras i tillhörande riktlinjer för områdena informationssäkerhet, säkerhet, säkerhetsskydd, krisberedskap samt civilt försvar, och kompletteras av Region Stockholms övriga styrande dokument.

I riktlinjerna regleras bland annat leverantörsrelationer. Bland annat pekas ut att regionens informationstillgångar måste ha samma skydd även om de hanteras av en leverantör. För att detta ska uppnås tydliggörs på ett övergripande plan hur arbetet med kravställning, upprättande och förvaltning av avtal samt hur riskhantering av leverantörsberoenden. Bland annat framgår att det inför varje upphandling ska göras en analys av vilka krav som behöver ställas, att upphandlande nämnd ska följa upp informationssäkerheten samt att åtgärder ska vidtas för att minska eventuella konsekvenser i det fall en leverantör inte kan fullfölja ett avtal.

I vägledningen Säkerställande av informationssäkerhet vid upphandling och avrop ges mer detaljerade råd kring bland annat analys inför upphandling, avtalsskrivning och ansvar för uppföljning under avtalets löptid. Vägledning till riktlinjer för informationssäkerhet ger också mer detaljerade råd. Vidare finns även Vägledning för riskhantering informationssäkerhet som syftar till att beskriva ett arbetssätt för hur informationssäkerhetsrisker kan bedömas och hur riskreducerande åtgärder kan hanteras.

Vägledningen Region Stockholms Compliance-process för informationssäkerhet syftar till att stödja nämnder och bolag att verka i enlighet med gällande policy och riktlinjer för informationssäkerhet. Genom att tillämpa compliance-processen kan avvikelser och brister upptäckas i ett tidigt skede och den faktiska informationssäkerheten i Region Stockholms verksamheter och IT-miljöer förbättras.

Det senast tillkomna styrdokumentet är vägledningen för systematiskt arbete med informationssäkerhet. Vägledningen syftar till att ge en enhetlig bild av hur informationssäkerhetssamordnarna vid Region Stockholms nämnder och bolag ska arbeta för att bedriva ett systematiskt informationssäkerhetsarbete. Målgruppen för vägledningen är informationssäkerhetssamordnarna vid respektive nämnd och bolag i Region Stockholm. Slutligen finns även Vägledning: Hjälp verksamheten att hantera information säkert och stärka säkerhetskulturen.

Iakttagelser; Intervjuer

De intervjuade beskriver att de i stor utsträckning följer de dokumentmallar som finns och den process som beskrivs i Avtalshandboken. De litar på att mallarna är avstämda med specialister och det är sällan det förekommer specifika diskussioner om krav avseende informationssäkerhet inför upphandling. Arbetssättet innebär dock att avtalsansvariga i praktiken avgör när en mall är lämplig att använda fullt ut, eller formuleringar i en mall, och när det behöver göras avvikelser eller anpassningar.

Detta uttrycker man under intervjuerna att man anser utgöra en viss brist, eftersom de avtalsansvariga inte anser sig ha tillräcklig kompetens för den typen av avvägningar, utan skulle behöva mer stöd av specialister. Det beskrivs att specialistkompetens i form av informationssäkerhetsspecialister eller jurister relativt sällan deltar i arbetet med att ta fram upphandlingsunderlag.

Iakttagelser; Upphandlingsunderlag

Upphandlingsunderlagen som granskats är från olika tidsperioder. Vårdval specialiserad hudsjukvård har underlag från 2019 och maj 2022, upphandlingen av närakut innerstaden är från 2019 och vårdval barn- och ungdomsmedicin har ett underlag från juni 2022. I alla underlagen ställs kravet att vårdgivarna ska följa lagar, förordningar och föreskrifter, de vid var tid gällande policies och riktlinjer avseende informationssäkerhet som beslutas om av Region Stockholm, att informationsskyddet ska dokumenteras samt att den informationen ska kunna delges Region Stockholm på begäran.

I övrigt skiljer sig underlagen lite åt avseende kravnivå. Exempelvis är kravställningen för vårdval specialiserad hudsjukvård från maj 2022 tämligen summarisk och hänvisar endast till att regionens styrande dokument på området ska följas, samt att informationsskyddet ska dokumenteras och kunna uppvisas på begäran. Underlaget för barn- och ungdomsmedicin, från juni 2022, har en betydligt mer fyllig kravbeskrivning. Exempelvis beskrivs att vårdgivaren behöver ha robusta och säkra informationssystem, ett ledningssystem för informationssäkerhet ska finnas och en rutin för att kunna identifiera informationssäkerhetsrelaterade risker ska finnas på plats.

I samtliga underlag framgår att vårdgivaren har rätt att bli ansluten till regionens gemensamma kommunikationsnätverk, SLLNET. Det framgår däremot inte vilka krav

som ställs på vårdgivaren för att ansluta. Dessa framgår indirekt och på en översiktlig nivå genom att de framgår av Riktlinjer för informationssäkerhet, vilka vårdgivaren är skyldig att följa.

Bedömning

PwC bedömer att regionens styrdokument i allt väsentligt har det innehållet som krävs utifrån regelverk och praxis. Eftersom regionens egna styrande dokument utgör den huvudsakliga delen av kraven avseende informationssäkerhet gör PwC bedömningen att regionen utifrån ett översiktligt perspektiv ställer ändamålsenliga krav.

Dock är det inte helt tydligt, eller konsekvent uttryckt i de olika avtalen, om det är de övergripande styrdokumenten som utgör krav gentemot vårdgivarna, eller om det är samtliga styrande dokument. På vårdgivarguiden.se finns dessutom ytterligare styrande dokument (exempelvis HSF:s Informationssäkerhetsanvisningar för vårdgivare som ansluter mot Region Stockholms nätverk (SLLNET)). Det är uppenbart att dokumenten på vårdgivarguiden är avsedda att vara styrande gentemot vårdgivarna, men det är tveksamt om de krav som uttrycks där i alla lägen kan sägas utgöra bindande krav och avtalsvillkor gentemot vårdgivarna.

I avtalet för vårdval barn- och ungdomsmedicin finns ett avsevärt förtydligande avseende frågan om vilka styrande dokument vårdgivaren är bunden av. I det avtalet hänvisas till att all information och alla anvisningar som finns på vårdgivarguiden.se utgör krav och villkor som är en del av avtalet. Skillnaden i avtalsskrivning innebär en relativt stor förbättring avseende vilken möjlighet regionen har att genomdriva exempelvis sanktioner kopplat till brister i efterlevnad av andra styrande dokument förutom de som explicit nämns i avtalen.

När det gäller momenten kvalificering och utvärdering, kan vi dock inte se att kraven från styrdokumenten finns med. Kvalificering och utvärdering utgår i huvudsak från ekonomisk stabilitet, laglydighet, förmåga att bedriva den aktuella vården och kvalitetsaspekter på densamma. Kraven avseende informationssäkerhet formuleras genom avtalsvillkor. Dessa blir ett indirekt “krav” i och med att godkännande av avtalsvillkoren är en förutsättning för att kunna lämna anbud/ansökan.

Tillvägagångssättet innebär dock att en potentiell vårdgivares förmåga att följa de aktuella styrdokumenten, om vårdgivaren är införstådd med vad kraven konkret innebär samt hur de tillämpas i eventuell befintlig verksamhet (alternativt hur de planeras att tillämpas), aldrig egentligen prövas innan tilldelningsbeslut/godkännande och därefter avtalsskrivande. Vilket i sin tur innebär att de krav 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 självklart en risk att regionen inte lever upp till sitt lagstadgade åtagande (utifrån att informationssäkerhet idag har ett tätt samband med kontinuitet i leverans) och det kan även innebära risker för den enskilde patienten.

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 leder till merarbete, sänkt vårdkapacitet och kanske till och med kvalitetsbrister för regionen.

Vi vill också lyfta fram skillnaden i att styra en egen verksamhet genom styrande och stödjande dokument, och att genom upphandling styra en extern verksamhet att leverera en önskad tjänst på ett önskat sätt. Styrdokumenten är skrivna för den egna verksamheten, utifrån dess organisation, begrepp, flöden och så vidare. De är också skrivna utifrån att vara vägledande till en given konkretiseringsnivå, därefter ska verksamheterna själva ansvara för att ta fram exempelvis rutiner eller ett specifikt tillvägagångssätt.

Till viss del går detta att överföra till styrning av leverantörer, men inte helt och hållet. Ett exempel är att styrning av leverantörer behöver utgå ifrån mätbara leveranser/effekter/förmågor oberoende av leverantörens organisation, flöden och så vidare för att avtalsmässigt vara användningsbara. Ett annat är att kraven på en leverantör ofta behöver ställas i relation till en risknivå för den tjänst/vara som upphandlas för att få en bra balans mellan pris och kvalitet. Det innebär att kraven kan behöva variera och ibland vara relativt övergripande, till att vara mycket detaljerade. För regionen skulle man exempelvis kunna identifiera anslutning till SLLNET som en hög risk, vilket innebär att det kan finnas skäl för att ställa specifika krav kopplat till just anslutningen.

Revisionsfråga 2: Har HSN en ändamålsenlig metod för att de identifierade kraven i punkt 1 säkerställs genom hela upphandlingsprocessen?

Iakttagelser; Intervjuer

Under intervjuerna beskrivs att respektive projektgrupp för en upphandling ansvarar för att projekten fortskrider som de ska. Styrgrupperna ansvarar för att hantera strategiska frågeställningar, och principiella frågor VBU. De intervjuade anser att det finns utvecklingspotential i det samarbetet, exempelvis när det kommer till intresseavvägningar. Man anser att det skulle behöva avsättas mer tid till den typen av diskussioner och bedömningar än vad som sker.

Det beskrivs att avtalsmallen och metodiken för upphandlingarna kontinuerligt följs upp av särskilda avtalsgrupper som består av representanter från alla avdelningar samt av avdelningschefer och representanter från olika typer av styrgrupper. Informationssäkerhetssamordnarna uppger dock att de inte är involverade i detta arbete. Samordnarna är inte heller en del av nätverket Noden som kvalitetssäkrar upphandlingsunderlag utifrån ett IT-perspektiv.

Det uppges vidare att man är trygg med arbetssättet men samtidigt ser att kraven som ställs har sitt ursprung i ett relativt traditionellt sätt att se på hälso- och sjukvård. Exempelvis lyfts det fram att regionen i större utsträckning borde ställa krav på effektivisering, utveckling och förbättringsarbete hos de externa vårdgivarna. Å andra sidan lyfts det även fram att kravställningen kopplat till informationssäkerhet har utvecklats sista åren. Det beskrivs också att arbetet med att fånga upp erfarenheter och läranden från en upphandling till nästa, i stor utsträckning vilar på den enskilde medarbetaren. I vissa fall samlas erfarenheter i dokument som förs vidare, men oftast bygger lärandet på att det är samma personer som arbetar med efterföljande upphandlingar.

Under intervjuerna beskrivs också att även om det i styrdokumenten ställs krav på specifika riskbedömningar och avvägningar inför varje upphandling, sker det i relativt liten utsträckning i praktiken. Oftast används de olika malldokumenten och det förutsätts att mallarna är uppdaterade med relevanta krav och villkor. Det uttrycks att samarbetet med sakkunniga inför upphandlingar är relativt litet i omfattning, vilket framhålls som en brist. Under intervjuerna framförs även för att man anser att det inom ramen för arbetet med att upphandla vård, behöver tillföras mer kompetens inom området informationssäkerhet.

Bedömning

Den process som beskrivs i Avtalshandboken bedöms som i allt väsentligt ändamålsenlig eftersom den bygger på kvalitetssäkrade standarddokument, det ska göras ändamålsenliga anpassningar för de specifika upphandlingarna samt att avstämningspunkter är beskrivna både avseende förankring och beslutsfattande. Avtalshandboken med tillhörande stödjande dokument utgör dessutom i sig självt ett omfattande och gediget stödmaterial.

Däremot verkar inte processen, i praktiken, riktigt gå till som den beskrivs i teorin utifrån att det under intervjuerna beskrivs ett arbetssätt som i relativt stor utsträckning utgår

ifrån de mallar som tillhandahålls, och där det i realiteten inte görs några betydande riskanalyser eller liknande. Intervjuerna ger även vid hand att informationssäkerhetssamordnarna i realiteten inte är involverade i arbetet med att skapa upphandlingsunderlag eller att följa upp befintliga avtal i någon större utsträckning eller på ett systematiskt sätt.

Redogörelserna stöds av hur upphandlingsunderlag/avtal är utformade, där krav och villkor avseende informationssäkerhet, i allt väsentligt är likartade. Att kraven och villkoren till största del är likartade behöver inte vara negativt; i stor utsträckning styrs ju de upphandlade tjänsterna av samma lagkrav och praxis. Men de olika typerna av upphandlad vård skiljer sig ändå avsevärt åt avseende exempelvis deras betydelse för regionen att leva upp till deras lagstadgade åtagande och hur känslig verksamheten är utifrån ett patientsäkerhetsperspektiv. Det innebär att det också är rimligt med olika riskbedömningar för olika typer av upphandlad vård, och därmed olika nivåer på kravställningen.

Utifrån intervjuerna bedömer vi även att det till viss del saknas en metodik för det organisatoriska lärandet. Strukturen är tydlig och stödmaterialet är omfattande avseende planerings- och genomförandefaserna, men inte lika tydligt när det gäller fasen att hämta in, strukturera och tillgängliggöra erfarenheter och läranden. Bristen innebär en risk för att utvecklingen av verksamheten går långsammare än nödvändigt och kan i värsta fall innebära en risk för att likartade fel, brister eller misstag upprepas.

Implementering av upphandlingskrav i efterföljande avtal

Revisionsfråga 3: Har HSN implementerat de identifierade kraven på ett ändamålsenligt och effektivt sätt i avtalen med de upphandlade leverantörerna?

Iakttagelser; Granskning upphandlingsunderlag och avtal

Närakuten innerstaden

På flera sätt framgår det som ett allmänt villkor i avtalet, att vårdgivaren enligt avtalet är skyldig att följa tillämpliga konventioner, lagar, föreskrifter, samt Region Stockholms egna policies och riktlinjer. I det fall en vårdgivare inte skulle följa det villkoret finns i huvudsak tre sanktionsmöjligheter;

1. Vårdgivaren kan få betala vite tills bristen är rättad.
2. Regionen kan säga upp avtalet med viss uppsägningstid om rättelse inte vidtas.
3. Om bristen är väsentlig kan regionen säga upp avtalet med omedelbar verkan.

Om regionen har beslutat om vite kan detta kvittas mot ersättning som regionen skulle ha betalat ut till vårdgivaren. I övrigt innehåller avtalet inga sanktioner eller påföljder kopplat till brister avseende informationssäkerhet.

Avtalets system för ersättning bygger på flera olika parametrar där fast ersättning kombineras med bonus kopplad till måluppfyllelse och prisavdrag och viten kopplat till brister i efterlevnad av avtal och utlovad kvalitetsnivå. Ingen del i ersättningssystemet berör informationssäkerhet vilket innebär att det inte finns några ekonomiska incitament

för vårdgivaren att öka kvalitetsnivån eller utveckla arbetssätt och skyddsnivåer avseende informationssäkerhet.

Av avtalet framgår också att vårdgivaren ska skydda sin information mot otillbörlig åtkomst och förstörelse. Hur man gör detta ska dokumenteras och dokumentationen ska kunna visas upp på begäran. Det framgår också att vårdgivaren ska använda sig av verktyg och åtgärder som ska hindra att information läcker ut, förvanskas eller förstörs, men möjliggör att informationen är tillgänglig när det behövs.

I avtalets Allmänna villkor anges att vårdgivaren ska se till att all dess personal och uppdragstagare (inklusive anställda och uppdragstagare hos vårdgivarens leverantörer) omfattas av samma regler om tystnadsplikt som hälso- och sjukvårdspersonal. Det anges även att vårdgivaren måste tillse att patientuppgifter skyddas så att obehöriga inte får åtkomst till dem, exempelvis får de inte skickas på öppna nät och åtkomst ska medges genom stark autentisering.

Vårdgivaren ges en ensidig rätt i avtalet att få ansluta till SLLNET, regionens kommunikationsnätverk men det ställs inga uttryckliga krav på vårdgivaren för att få ansluta. Dessa finns beskrivna på Vårdgivarguiden i form av ett policydokument men framkommer inte i avtalet.

Avtalet ger regionen i princip en oinskränkt rätt att göra olika typer av uppföljningar och revisioner av hur avtalet efterlevs.

Vårdval specialiserad hudsjukvård, 2019 och 2022

Avseende informationssäkerhet är villkoren i dessa avtal liknande de för närakut innerstaden.

I båda avtalen ställs krav på att vårdgivaren ska dokumentera hur man skyddar information och att den dokumentationen ska kunna visas upp för regionen. I 2019 års avtal förtydligas vad dokumentationen ska innehålla, men till 2022 års avtal är det förtydligandet borttaget.

Villkoren kopplat till vite vid brister i utförandet är något annorlunda utformade jämfört med närakut innerstaden, men till sin funktion bedöms de ha samma eller likartad effekt.

Vårdval barn- och ungdomsmedicin

Avseende informationssäkerhet är strukturen och till viss del innehållet i detta avtal liknande de för närakut innerstaden och vårdval specialiserad hudsjukvård. Däremot är villkoren utvecklade i riktning mot att ställa tydligare och högre krav på vårdgivare. Bland annat krävs att vårdgivare har ett ledningssystem som motsvarar SOSFS 2011:9 och vårdgivare har även en skyldighet att kunna visa upp dokumentation som stödjer att de nämnda kraven i avtalet är uppfyllda.

Skrivningen avseende att vårdgivarna ska säkerställa ett sekretesskydd motsvarande det som gäller för regionen finns inte med i detta avtal.

I det fall vårdgivare inte uppfyller kraven avseende informationssäkerhet har det i detta avtal införts en möjlighet för regionen att stänga av digitala tjänster och anslutningar som regionen tillhandahåller. Regionen ges också möjlighet att omedelbart avsluta avtalet om det visar sig att vårdgivaren vid driftstart inte kan uppfylla de åtaganden man har enligt avtalet. I övrigt är principerna för påföljder vid bristande avtalssuppfyllelse, liknande övriga jämförda avtal, med skillnaden att de generellt är skarpare till vårdgivarnas nackdel.

Bedömning

Närakuten innerstaden och vårdval specialiserad hudsjukvård

De allmänna kraven att vårdgivaren ska följa gällande lagar, regler och regionens vid var tid gällande policies bedömer vi vara ett tydligt grundläggande villkor. I de mer specificerade villkoren används ordval som ”otillbörlig” (det vill säga ”olämplig” eller ”opassande”) åtkomst, att vårdgivaren ”ska använda sig av verktyg som ska hindra exempelvis läckage”, samt att vårdgivaren ska ”möjliggöra” att information är tillgänglig när den behövs. Sammantaget innebär detta relativt flexibla villkor för vårdgivaren som inte är likvärdiga med krav i lagstiftningen.

Ett alternativ hade kunnat vara att vårdgivaren behöver garantera att ingen ”obehörig” får tillgång till information, att inget informationsläckage får ske samt att information ska vara tillgänglig när den behövs. Sådana skrivningar skulle bättre motsvara kraven i lagstiftning, samt vara mer rimlig utifrån hur känslig informationen i detta sammanhang kan vara, och hur angeläget det kan vara med tillgång vid rätt tillfällen. Utifrån ett affärsmässigt perspektiv skulle den typen av skrivningar också ge regionen ett bättre utgångsläge att exempelvis kunna visa på brister som grund för prisavdrag och så vidare.

En tydligare reglering avseende kraven för att få ansluta till SLLNET hade varit att föredra. Eftersom kraven framkommer i ett styrande dokument, och vårdgivarna är skyldiga att följa dessa, omfattas sannolikt de externa vårdgivarna av det styrande dokumentet. Men eftersom dokumentet inte namnges eller tydliggörs i avtalet riskeras en situation där det finns ett bindande avtal, och en tydlig rätt (och rimligtvis en förväntan) för vårdgivaren att få ansluta, men i värsta fall en bristande förmåga hos densamme. Det innebär att det finns risk för en situation där vårdgivaren i praktiken inte kan bli ansluten till SLLNET, men där vårdgivaren har en avtalsmässigt bindande rätt att få bli ansluten. Den typen av situationer skapar merarbete och risk för att avtal behöver brytas.

Det är positivt att kvittningsmöjlighet avseende vite finns. Risken för utebliven ersättning ökar generellt sett incitamenten att följa avtalet, och förenklar dessutom administrativa processer. Det är också positivt att regionen har så stora möjligheter till uppföljning och revision eftersom det ger formella förutsättningar för en god och effektiv uppföljning.

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

De vitesmöjligheter som regionen har i det fall allmänna brister kan konstateras 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 (eftersom avtalen är så allmänt skrivna 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.

Vårdval barn- och ungdomsmedicin

Eftersom detta avtal i grunden är likartat de övriga granskade avtalen är även bedömningen i stor utsträckning densamma.

De skillnader som finns i detta avtal innebär i princip odelat en större möjlighet för regionen att driva igenom följsamhet till interna styrdokument och lagkrav. Möjligheten att stänga av en vårdgivare från digitala tjänster och nätverk är ett exempel på en åtgärd som kan verkställas snabbt och är relativt enkel att administrera. Anslutningen är dessutom sannolikt viktig för vårdgivarna, vilket innebär att en risk för avstängning utgör ett starkt incitament för vårdgivaren att följa avtal och regelverk. Det är också en sanktion som på ett rimligt sätt avspeglar den risk för regionens IT-miljö som en anslutande vårdgivare kan utgöra.

Faktumet att skrivningen om att vårdgivaren ska tillförsäkra att dess personal ska omfattas av samma tystnadsplikt som hälso- och sjukvårdspersonal är en förenkling som minskar risken för motsägande regleringar i avtalet kontra lagstiftning. Frågan om tystnadsplikt avseende bland annat hälsouppgifter för enskilda är reglerat i lag, både för offentliga och externa vårdgivare.

Skrivningen i avtalen avseende Närakut innerstaden och Vårdval specialiserad hudsjukvård stämmer inte riktigt överens med lagtexten, vilket riskerar att leda till onödiga komplikationer. Därför är det bättre att endast hänvisa till lagstiftning och inte försöka ”dubbelreglera”.

Uppföljning av upphandlingskrav och avtalsvillkor

Revisionsfråga 4: Följer HSN upp att de avtalade kraven och villkoren följs av leverantörerna på ett ändamålsenligt sätt?

Nuvarande arbetssätt avseende avtalsuppföljning

Processen för att följa upp externa vårdgivare finns beskriven i Avtalshandboken. Uppföljningen planeras internt på förvaltningen. Uppföljningsplanen kan ändras under avtalsperioden, så länge avtalet tillåter och uppföljningen inte påverkar avtalets övergripande karaktär. Uppföljningens frekvens och omfattning bestäms utifrån en prioriteringsmodell för avtalsuppföljning som HSF beslutat om. Varje avtalsområde bedöms enligt särskilda kriterier och bedömningen ger ett utfall där olika avtalsområden placeras i olika grupper, utifrån prioritering.

Själva uppföljningen utförs genom att en mängd olika data samlas in, såsom ekonomiska uppgifter, väntetider, ärenden i patientnämnden, enkäter eller uppgifter kopplat till målrelaterad ersättning.

När datan är insamlad sammanställs den och analyseras. I det fall avvikelser, brister eller liknande upptäcks görs en bedömning hur detta ska hanteras och om påföljd kan vara aktuell. Ibland ger inte ordinarie avtalsuppföljning tillräckligt med information och i sådana fall kan en fördjupad uppföljning initieras.

En fördjupad uppföljning är ett komplement till ordinarie avtalsuppföljning och görs sällan utan att en ordinarie uppföljning först genomförts. I Avtalshandboken ges exempel på när en fördjupad uppföljning kan vara aktuell; exempelvis patientsäkerhet, misstanke om fusk eller felaktigt utbetalda ersättningar eller om det finns ett behov hos HSF att skapa sig själv ett kunskapsunderlag inför exempelvis en avtalsrevidering. Fördjupade uppföljningar kan även genomföras planerat, och bestäms då av HSF utifrån en risk- och väsentlighetsanalys.

Resultatet av uppföljningen kan sammanställas i en årsrapport, och i de fall det efterfrågas presenteras för HSN. Även andra typer av återkoppling/återföring anges i Avtalshandboken, samtliga med syfte att sprida information, kunskap och erfarenheter både inom regionen och utanför den egna organisationen.

Det är Avtalsstyrgrupperna som ansvarar för att kraven på informationssäkerhet efterlevs. Avtalsstyrgrupperna ligger under HSL-gruppen. På handläggarnivå är det den avtalsansvariga på beställaravdelningarna som ansvarar för att följa upp att leverantören uppfyller kraven och villkoren.

Iakttagelser; Styrande dokument

De övergripande kraven avseende uppföljning framgår av Region Stockholms riktlinjer. Mer detaljerade råd och rekommendationer återfinns i vägledningarna till riktlinjerna.

Av riktlinjerna framgår att i de fall nämnder och bolag uppdrar åt andra att hantera information ska avtalet om denna hantering omfatta sådana krav att informationen hanteras i enlighet med dessa riktlinjer. Den nämnd eller det bolag som avtalar med annan om hantering av information ansvarar också för en uppföljning av utförandet och de avtal som ligger till grund för utförandet, så att informationen ges ett avtalsenligt skydd.

Nämnder och bolag ansvarar för att uppföljning sker gällande hur leverantörer de har avtal med hanterar informationssäkerheten. Varje nämnd och bolag ska regelbundet genomföra revision av sin informationssäkerhet och göra en analys av hur skyddsåtgärder förhåller sig till gällande styrande regelverk samt aktuell hotbild. Baserat på genomförda granskningar och identifierade avvikelser ska skyddsåtgärder vidtas, anpassas och kompletteras.

Varje år ska nämnder och bolag följa upp status på informationssäkerheten inom det egna ansvarsområdet. Regionstyrelsen ska årligen utvärdera informationssäkerheten och verkan av det övergripande ledningssystemet för informationssäkerhet inom Region Stockholm.

Iakttagelser; Intervjuer

Under intervjuerna framkommer att det arbetssätt avseende uppföljning som beskrivs i Avtalshandboken, är väl känt och etablerat. Det är de avtalsansvariga som ansvarar för uppföljningen och den genomförs utifrån de uppföljningsplaner som finns inom avtalsområdet. De intervjuade beskriver även en utveckling av det systematiska arbetssättet avseende uppföljning och hur det har utvecklats från en relativt låg nivå till att bli mer och mer systematiskt och datadrivet.

Det beskrivs att de flesta avtalsansvariga har många avtal att följa upp (kan vara upp mot hundra i vissa fall), och därför görs hårda prioriteringar. Det påpekas också att de avtalsansvariga inte har de specialistkunskaper inom exempelvis informationssäkerhet som de själva anses krävs för att själva initiera den typen av uppföljning eller för att själva kunna bedöma det som eventuellt kan framkomma vid uppföljning.

Sammantaget innebär detta att det under intervjuerna inte kan ges exempel på granskningar av informationssäkerhet som gjorts utan förekommen anledning förutom i ett fall.[2] De handfull exempel på granskningar som ges kommer utifrån exempelvis incidenter eller där den avtalsansvarige har funnit anledning till extra kontroll i samband med driftstart eller annan uppföljning.

Det uppges samtidigt att även om en direkt uppföljning inte sker, kommer brister avseende informationssäkerhet ändå upptäckas förr eller senare, utifrån olika typer av tekniska krav och rapporteringskrav, som ställs för att vårdgivaren alls ska kunna leverera den avtalade tjänsten.

Under intervjuerna framkommer inga exempel på att resultaten av uppföljningar (exempelvis de årsrapporter som nämns i Avtalshandboken) efterfrågas av HSN eller delges nämnden på annat systematiskt sätt. Uppföljning är heller inte något som de intervjuade känner till ingår i nämndens interna kontroll (vilket bekräftas åtminstone avseende internkontrollplan 2022, där uppföljning av avtal och informationssäkerhet inte finns med som kontrollmoment)

Upphandlingsunderlag/Avtal

Uppföljning av informationssäkerhet hos vårdgivarna finns inte med i någon av de förbestämda uppföljningsplanerna för de utvalda avtalen för denna granskning.

Ny modell för särskild uppföljning av informationssäkerhet

Sedan 2019 har regionen utrett hur uppföljning av informationssäkerhet hos de externa vårdgivarna kan utvecklas, och i december 2022 fastslogs utredningens slutrapport genom beslut i projektets styrgrupp. Målet med utredningen har enligt slutrapporten varit ökad patientsäkerhet genom att vårdgivarna i högre utsträckning följer gällande lagstiftning inom området. För att nå dit har ett annat mål med utredningen varit att utveckla en metod och modell som HSF kan använda för att följa upp de externa vårdgivarna.

[2] Granskning av vårdgivaren Digital Medical Supply Sweden AB:s informationshantering är i enlighet med lag och ingångna avtal, 2021-02-19, dnr 2020-1776.

Metoden innebär, översiktligt beskrivet, att 68 frågor i en enkät ska besvaras av vårdgivaren. Svaren ska bedömas av avtalsansvarig utifrån en mall, och det finns även en mall framtagen för återkoppling till vårdgivarna. Svaren kan sedan användas som underlag för fördjupad uppföljning och eventuella vidare åtgärder. HSF:s plan för att etablera den nya metoden är att enkäten ska börja användas i begränsad omfattning under 2023, utvärderas vidare, och därefter planeras användningen att successivt skalas upp.

Frågorna i enkäten omfattar en mängd olika områden inom ramen för informationssäkerhet. Allt från om vårdgivaren har ett ledningssystem för informationssäkerhet, hur informationssäkerhet rapporteras till vårdgivarens ledning, vilka rutiner som finns för exempelvis incidenter och testning, om stickprov av loggar görs, om man kontrollerar att vårdgivarens leverantörer lever upp till sina åtaganden och om det är säkerställt att journaler bevaras i enlighet med regler och att de är läsbara hela denna tid.

Bedömning

Utifrån det material PwC fått tillgång till och genom intervjuerna gör vi bedömningen att regionen inte följer upp informationssäkerheten hos externa vårdgivare, mer än i enstaka fall och på förekommen anledning. De formella möjligheterna genom styrande dokument och ändamålsenliga avtalsvillkor finns på plats, och det finns en struktur för uppföljning där informationssäkerhet hade kunnat inkluderats.

Bristen på kontroll gör också att vi bedömer att HSN inte följer upp sina leverantörsrelationer på sådant sätt som både interna styrdokument och lagstiftning kräver. Vilket i sin tur innebär 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 HSN:s agerande, eller på grund av att krisåtgärder behöver sättas in om externa vårdgivare drabbas av produktionsbortfall.

Den nya modellen för uppföljning av informationssäkerhet är ett steg i rätt riktning, förutsatt att den implementeras i bred utsträckning och att resultatet tas om hand på ett ändamålsenligt sätt. Dock gör PwC bedömningen att även med den nya modellen, finns behov av reell, faktisk och fysisk kontroll av vårdgivares informationssäkerhet. Enkätfrågorna i den nya modellen är bra, men de ger inte en objektiv och säker bild över om den aktuella vårdgivaren faktiskt följer krav och avtalsvillkor.

Exempelvis rör flera av enkätfrågorna om olika typer av rutiner finns. En vårdgivare kan svara jakande på frågan om en rutin finns, men svaret kommer inte ge regionen någon information om rutinen följs eller om rutinen håller den kvalité som lagstiftning, avtal eller branschstandard/praxis kräver. Ett annat exempel är frågor som inkluderar en värdering, exempelvis ”Förvarar ni säkerhetskopior på ett säkert sätt, väl åtskilda från originaluppgifterna”. Så länge frågan inte kopplas till en definition av vad som utgör ”säkert sätt” och ”väl åtskild” kommer inte svaret på frågan ge regionen tillförlitlig information om vare sig lagstiftning, avtal eller ”best practice” följs av vårdgivaren.

Exempel på annan typ av avtalsrevision och uppföljning 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 HSLF-FS 2016:40 följs,
- Simulation av incidenter, penetrationstest eller liknande för att testa hur leverantörens skydd och arbetssätt fungerar i praktiken.

Revisionsfråga 5: I det fall avvikelser upptäcks, har HSN ett ändamålsenligt sätt att hantera dessa avvikelser?

Iakttagelser; Styrande dokument

Av riktlinjerna för informationssäkerhet framgår att varje nämnd och bolag regelbundet ska genomföra revision av sin informationssäkerhet och göra en analys av hur skyddsåtgärder förhåller sig till gällande styrande regelverk samt aktuell hotbild. Baserat på genomförda granskningar och identifierade avvikelser ska skyddsåtgärder vidtas, anpassas och kompletteras.

I Avtalshandboken finns ett avsnitt där det beskrivs hur brister, avvikelser och avtalsbrott ska hanteras. Det finns generella instruktioner, såsom att det är viktigt att agera skyndsamt vid upptäckt, att vara noga med att dokumentera samt att följa respektive avtals villkor avseende hur brister ska hanteras. Det finns även en beskrivning av en påföljdstrappa, där olika typer av åtgärder och sanktioner beskrivs, från meddelande till leverantör till viten och till sist avslut av avtal och i vissa fall även polisanmälan eller anmälan till IVO. I handboken beskrivs även utförligt hur medarbetaren ska gå till väga för att genomföra de olika påföljderna.

Iakttagelser; Intervjuer

Vid intervjuerna beskrivs att man är medveten om den sanktionstrappa och de arbetsrutiner som finns i Avtalshandboken. Man beskriver också medvetenhet om att alla upphandlingsunderlag innehåller lite olika möjligheter och metodiker vilket gör att arbetet med brister och avvikelser behöver anpassas utifrån respektive upphandlingsunderlag.

Alla intervjuade beskriver hur användandet av varningsbrev och i viss mån innehållande av ersättning/viten är relativt väl använda påföljder. Samtidigt beskriver man även en i allmänhet försiktig och restriktiv användning av starkare påföljder. Ingen av de intervjuade kan ge exempel på att en vårdgivare stängts av, att ett avtal sagts upp eller liknande, på grund av bristande informationssäkerhet. Däremot beskriver de intervjuade att man upplever ett större fokus på uppföljning, och att mer och mer arbete har genomförts för att skapa en struktur för att kunna effektuera påföljder, men även en viss attitydskillnad där försiktigheten har minskat.

Iakttagelser; Upphandlingsunderlag och avtal

<u>Närakut innerstaden</u>

Avtalsvillkoren ger regionen rätt att, i det fall man anser att vårdgivaren brister i efterlevnaden av avtalet (oaktat på vilket sätt eller inom vilket område), meddela

vårdgivaren en varning och bestämma en tidsplan för när bristen ska vara åtgärdad. Om bristen inte åtgärdas i tid har regionen rätt att ta ut ett vite. Samma princip för sanktion gäller om vårdgivaren brister i sin rapportering till regionen, eller rapporterar felaktigt som leder till en för hög ersättning. En tredje sanktionsmöjlighet föreligger om vårdgivaren brister i kvalitet. Dock är definitionen av kvalitet begränsad till de indikatorer som finns i den uppföljningsplan som biläggs avtalet, och där ingår inga indikatorer avseende informationssäkerhet.

I avtalet finns också reglerat i vilka situationer som regionen kan säga upp avtalet med omedelbar verkan. För det krävs väsentliga brister, och i avtalet exemplifieras vilka dessa kan vara. Inga exempel avser informationssäkerhet direkt, men däremot träffas området indirekt genom exemplet om vårdgivaren "åsidosätter bestämmelser i lagar, förordningar eller föreskrifter."

Det finns även en möjlighet för båda parter att säga upp avtalet, i det fall ena parten inte följt avtalet, och inte heller vidtagit rättelse inom 30 dagar.

Vårdval specialiserad hudsjukvård

Avtalsvillkoren avseende påföljder vid brister och avvikelser liknar i sin struktur och innehåll villkoren som gäller för Närakut innerstaden. Den största skillnad består i att regionen har rätt att innehålla upp till fem procent, vilket är en höjning jämfört med närakuten innerstaden, av den månatliga betalningen till vårdgivaren, i det fall den brister i efterlevnaden av avtalet.

Vårdval barn- och ungdomsmedicin

Avtalsvillkoren avseende påföljder vid brister och avvikelser liknar i sin struktur och innehåll villkoren som gäller för Närakut innerstaden. Vitesbeloppen är dock generellt högre och det förtydligas att flera påföljder kan aktualiseras för samma brist.

Det finns även ett särskilt villkor som relaterar till brister avseende informationssäkerhet och IT-säkerhet. Villkoret ger regionen en ovillkorlig rätt att stänga av vårdgivaren från användning eller anslutning till digitala tjänster och system som regionen tillhandahåller vårdgivaren inom ramen för det aktuella avtalet.

En annan väsentlig skillnad är att regionen i detta avtal har möjlighet att innehålla utbetalning av ersättning i det fall regionen anser sig ha krav på vårdgivaren i form av exempelvis viten eller återbetalning.

Bedömning

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 den avstängningsmöjlighet till tjänster och system som finns i avtalet för barn- och ungdomsmedicin. Eftersom anslutningen och användningen av regionens system i många fall är en förutsättning för en privat vårdgivare att kunna utföra sitt uppdrag innebär det självklart ett starkt incitament för vårdgivaren att följa avtalet. Det är också en effektiv åtgärd eftersom avstängningen kan göras omedelbart och helt ensidigt från regionens sida.

I de underlag vi granskat ser förutsättningarna för effektiva påföljder lite olika ut. Det äldsta avtalet, närakut innerstaden, ger relativt svaga möjligheter, medan det nyaste avtalet, barn- och ungdomsmedicin, ger bättre möjligheter. I det senaste avtalet är det även tydligare att det gjorts viss riskbedömning och att särskilda påföljdsmöjligheter har skapats utifrån den riskbedömningen.

Regionens riktlinje för informationssäkerhet ger en tydlig instruktion att varje nämnd är ansvarig för att både följa upp informationssäkerhet i sin egen verksamhet och hos leverantörer, samt agera på eventuella brister. Utifrån intervjuerna bedömer vi att ett sådant systematiskt arbetssätt ännu inte är etablerat. Vid de få fall av upptäckta avvikelser som har beskrivits under intervjuerna har det inte aktualiserats någon form av påföljd, utan avvikelserna har bestått i brister som kunnat åtgärdats. Det har heller inte beskrivits att avvikelserna har rapporterats till exempelvis ansvarig nämnd eller att de gett upphov till förändrade krav eller villkor.

Uppföljning av tidigare granskning av Regionrevisionen

Revisionen gjorde 2018 bedömningen att krav gällande informationssäkerhet och personuppgifter var tydligt formulerade i avtal med externa vårdgivare. Däremot bedömde man att HSN inte genomförde någon systematiserad och dokumenterad uppföljning för att säkerställa att kraven efterlevs. Revisionen rekommenderade HSN att snarast skapa rutiner för uppföljning av informationssäkerhet gentemot externa vårdgivare.

Utifrån det material som vi fått tillgängligt och de intervjuer som genomförts kan vi inte se att granskningar av informationssäkerhet har genomförts i större omfattning än tidigare, eller att en systematik etablerats. Bland de intervjuade är det dock tydligt att medvetenheten om både behovet och angelägenheten finns. I och med det nyligen avslutade projektet för att skapa en metod att följa upp informationssäkerhet har

förutsättningarna för att uppföljning ska ske förbättrats, men vi kan inte konstatera att ett förändrat arbetssätt är etablerat.

I HSN:s verksamhetsplan för 2022 finns även angivet att avtal och uppföljning inom området ska förtydligas. Detta bekräftas till viss del i upphandlingsunderlag/avtal för vårdval barn- och ungdomsmedicin, men samtidigt syns inte riktigt tecken på denna ambitionshöjning i det för 2022 års uppdaterade upphandlingsunderlag/avtal för vårdval specialiserad hudsjukvård.

Sammanfattningsvis görs bedömningen att avtal till viss del har förtydligats, och att en ansats till utvecklad och mer omfattande uppföljning finns, vilket får ses som en positiv utveckling.

2023-01-15

REBECKA HANSSON CHARLOTTE ARNELL

Vad gör regionrevisorerna?

Regionrevisorerna granskar den verksamhet som bedrivs av regionens nämnder och bolagsstyrelser. Revisionsuppdraget är det största inom kommunal verksamhet.

Att vara revisor är ett förtroendeuppdrag vars syfte är att med oberoende, saklighet och integritet främja, granska och bedöma verksamheten. Den övergripande uppgiften för revisorerna är att granska hur nämnder och styrelser tar sitt ansvar. De förtroendevalda revisorerna är fullmäktiges och ytterst medborgarnas instrument för den demokratiska kontrollen. De har därmed en viktig funktion i den lokala självstyrelsen.

Ledamöter i nämnder och styrelser ansvarar inför fullmäktige för hur de själva, anställda och uppdragstagare genomför verksamheten. I ansvaret ingår att genomföra en ändamålsenlig verksamhet utifrån fullmäktiges mål, beslut och riktlinjer samt de föreskrifter som gäller för verksamheten, på ett ekonomiskt tillfredsställande sätt och med en tillräcklig intern kontroll samt att upprätta rättvisande räkenskaper.

I årsrapporter för nämnder och styrelser sammanfattar revisionskontoret den granskning som genomförts under det gångna året. Verksamhetsrevisionen redovisas löpande i projektrapporter. Publikationerna presenteras på regionrevisorernas webbsida på www.sll.se. Det går även att prenumerera på regionrevisorernas nyhetsbrev Nytt från regionrevisionen genom att anmäla intresse via e-postmeddelande till landstingsrevisorerna.rev@sll.se.

Region Stockholm

Postadress: Box 22230, 104 22 Stockholm
Besöksadress: Hantverkargatan 25 b (T-bana Rådhuset)
Telefon: 08-737 25 00
E-post: landstingsrevisorerna.rev@sll.se
Hemsida: www.sll.se
Org.nr: 232100-0016