Hälso- och sjukvårdsförvaltningen

Granskningsrapport

Extern granskning avseende informationssäkerhet

20 juni 2019

Till Enhetschefen för enhet Verksamhetsplanering och uppföljning

Innehållsförteckning

1. Inledning

1.1 Bakgrund

Region Stockholm bär det övergripande ansvaret för att länets invånare ska få den hälso- och sjukvård de behöver, vilket innefattar att invånare ska kunna förlita sig på att den information de lämnar får ett tillräckligt skydd från obehöriga. Detta innebär bland annat för Region Stockholm att säkerställa att rätt krav ställs på vårdgivare som hanterar känslig information samt att avtalen följs upp på ett ändamålsenligt sätt.

Genom HSF har Region Stockholm avtal med vårdgivaren MedHelp AB (”Vårdgivaren”) gällande utförande av tjänsten 1177 Vårdguiden på telefon, tecknat i februari 2013. Den 18 februari 2019 framkom att inspelningar av vissa samtal till 1177 Vårdguidens sjukvårdsrådgivning på telefon varit tillgängliga över internet för obehöriga. Incidenten berodde på en felkonfigurerad lagringsenhet hos bolaget Medicall, en underleverantör till vårdgivaren MedHelp AB som hanterade samtal under kvällar, nätter och helger.

Med anledning av den allvarliga händelsen har Region Stockholm, genom HSF, uppdragit åt KPMG att genomföra en oberoende utredning gällande informationssäkerhet i tjänsten 1177 Vårdguiden på telefon.

1.2 Syfte med granskningen

Granskningens övergripande syfte har varit att granska HSF:s gällande avtal med Vårdgivaren för att tydliggöra huruvida kraven i avtalet och förvaltningens avtalsuppföljning har varit ändamålsenliga med avseende till området informationssäkerhet. Granskningen syftar även till att lämna övergripande bedömningar kring Vårdgivarens efterlevnad av avtalet.

Granskningen har omfattat tiden för avtalets tecknande gällande lagstiftning inom hälso- och sjukvårdsområdet samt lagstiftning i övrigt med de förändringar som skett fram till händelsen. Utöver regelefterlevnad har granskningen även utgått från relevanta delar av styrande dokument hos respektive part samt rådande standarder och praxis inom området informationssäkerhet.

Uppdraget har även inkluderat att lämna rekommendationer där vi identifierat förbättringsområden, vilket bland annat skulle kunna innefatta råd kring förtydligande av avtal, uppföljningsrutiner och processer för att minimera risken att motsvarande incidenter inträffar igen.

För att uppfylla granskningens syfte har vi arbetat utifrån följande revisionsfrågor:

- Är kraven i avtalet med avseende på informationssäkerhet ställda på ett rimligt sätt?
- Har den avtalsuppföljning som Region Stockholm bedrivit genom Hälso- och sjukvårdsförvaltningen varit relevant?
- Har Vårdgivaren etablerat och efterlevt de kvalitetssystem, processer, rutiner och tekniska skyddsåtgärder gällande informationssäkerhet som är rimliga utifrån lagkrav, avtalade krav och god praxis?

1.3 Granskningens genomförande och omfattning

Granskningen har omfattat en kombination av IT-revision, inhämtning av information från tillgänglig dokumentation av karaktären styr- och stöddokument, uppföljningsrapporter samt intervjuer med nyckelpersoner. Granskningen har utgått från vedertagna granskningsmetoder inom området informationssäkerhet, vilket omfattat såväl Vårdgivaren och dennes underleverantörer som Region Stockholm genom HSF. En lista över de personer som intervjuats återfinns i bilaga 2. Granskningen har genomförts under maj-juni 2019.

Vidare är rapportens utformning i avvikelseformat där endast väsentliga iakttagelser har lyfts fram med förslag på förbättringsåtgärder, inklusive eventuella behov att förtydliga avtal, uppföljningsrutiner och processer för att minimera att motsvarande inträffar igen.

2. Sammanfattande bedömning

Vår övergripande bedömning är att HSF bör se över kravställningen på informationssäkerheten i samband med upphandlingar samt att uppföljningsprocessen behöver struktureras och formaliseras för icke funktionella krav, däribland informationssäkerhet. I allt väsentligt behöver kravställningen preciseras för att säkerställa att leverantörerna är införstådda i HSF:s förväntningar, men även för att öka den interna förståelsen för hur kraven ska följas upp. Att avtalskraven beträffande informationssäkerhet är allmänt hållna, samtidigt som standarden inom området inte är fullt integrerad i HSF:s verksamhet, innebär i praktiken att Vårdgivarens hantering av informationssäkerhet endast har följts upp i begränsad omfattning.

Vad gäller Vårdgivaren kan vi konstatera att det inte finns något dokumenterat ledningssystem för informationssäkerhet samt att det förekommit brister i rutinen för utvärdering och uppföljning av underleverantörer till vårdtjänsten. Vi noterar dock att Vårdgivaren, sedan incidenten, arbetar med en åtgärdsplan för att förbättra informationssäkerheten, rutiner beträffande kontroll av leverantörer samt planerar för en certifiering inom ISO 27001.

Vi noterar att de akuta bristerna hänförliga till incidenten har hanterats, bland annat genom den skyndsamma nedstängningen av den felkonfigurerade servern, uppsägningen av avtalet med underleverantören som givit upphov till incidenten samt inhämtandet av all patientinformation till Vårdgivarens egen tekniska lösning. Vi har dock identifierat ett antal framåtblickande förbättringsområden som rör HSF:s övergripande arbetssätt beträffande informationssäkerhet, fördelningen av roller och ansvar samt metoden för hantering och uppföljning av leverantörer. Vidare har vi även identifierat åtgärder hänförliga till Vårdgivarens arbete med informationssäkerhet och den planerade ISO-certifieringen samt sättet till vilket Vårdgivaren arbetar med att vidareförmedla HSF:s avtalskrav beträffande informationssäkerhet.

I detta avsnitt redogör vi för våra samlade bedömningar hänförliga till de övergripande granskningsfrågorna. Bedömningarna sammanfattas i avsnitten *HSF:s kravställning i avtalsprocessen, löpande uppföljning av avtal* samt *Vårdgivarens efterlevnad av avtalsvillkor, lagar och regler samt god praxis.* I efterföljande avsnitt beskriver vi följaktligen väsentliga iakttagelser samt tillhörande rekommendationer.

2.1 Samlade bedömningar hänförliga till de övergripande granskningsfrågorna

2.1.1 HSF:s kravställning i avtalsprocessen

Att säkerställa potentiella vårdgivares leveranskapacitet ligger i hjärtat av en upphandling, men det är likväl viktigt att försäkra sig om deras förmåga till att bedriva en sund och säker verksamhet på sikt. Informationssäkerheten är i sammanhanget kritisk eftersom en god hantering ökar tryggheten vad gäller vårdgivarens förmåga till att säkerställa kontinuitet i verksamheten samt skydda de känsliga uppgifterna som hanteras inom ramen för vårdtjänster.

Utöver specificering av den upphandlade tjänsten har vi noterat att kravställningen utgår från två perspektiv – kvalificering och utvärdering. Vid kvalificering utgår kravställningen från ekonomisk stabilitet samt teknisk förmåga och kapacitet, medan utvärderingen utgår från prisfördelaktighet i förhållande till tjänstens utformning och innehåll. Övriga krav definieras genom allmänna villkor och standardiserade bilagor vilka är utformade på ett sådant sätt att de ska kunna appliceras i HSF:s samtliga avtal med vårdgivare. Vår bedömning är att kravställningen vad gäller icke funktionella krav, såsom intern kontroll och informationssäkerhet, är för allmänt hållna för att i sig kunna ge en trygghet i att vårdgivaren är införstådd samt tillämpar dem på ett

ändamålsenligt sätt. HSF utvärderar inte heller dessa aspekter under pågående upphandlingar som en del av den potentiella vårdgivarens samlade leveransförmåga. Vår bedömning är att HSF bör införa en riskbaserad ansats till sina leverantörer, vilket innebär att dessa kategoriseras enligt portföljprincipen samt att kravställningen följaktligen anpassas utefter deras vikt för verksamheten.

Förmågan att ställa ändamålsenliga krav på leverantörers hantering av informationssäkerhet har därutöver ett väsentligt beroende till HSF:s egen kapacitet och mognadsgrad kopplad till informationssäkerhet samt sättet till vilket denna kunskap integreras i verksamhetens processer. Vår bedömning är att HSF ännu inte har något fullständigt ledningssystem för informationssäkerhet samt att standarden därav inte är tillräckligt integrerad i verksamheten för att möjliggöra en relevant kravställning mot externa parter.

2.1.2 Löpande uppföljning av vårdavtal

Avtalsuppföljningen genomförs med fokus på kvalitetssäkringen av tjänsten, vilket vi bedömer fungerar väl. Uppföljningen sker dock inte utifrån en förutbestämd process, utan avtalshandläggarna har utformat uppföljningen baserat på konkreta och mätbara villkor i vårdavtalet. Avtalet, inklusive de allmänna villkoren, ger ett visst utrymme till att följa upp andra aspekter hos vårdgivaren och enligt uppgift sker sådan uppföljning baserat på avtalshandläggarens preferenser och kunskaper. Detta innebär dock i förlängningen att flertalet icke funktionella krav inte hanteras i proportion till deras vikt, vilket vi bedömer beror på svårigheten för icke-experter att tolka och applicera allmänt hållna avtalskrav på ett meningsfullt sätt inom ramen för en uppföljningsprocess. Vad gäller informationssäkerhet kan vi konstatera att viss uppföljning har gjorts beträffande Vårdgivarens införande av GDPR, men att uppföljningen därutöver inte har varit tillräckligt heltäckande eller strukturerad för att säkerställa en tillfredsställande hantering av känslig information.

2.1.3 Vårdgivarens efterlevnad av avtalsvillkor, lagar och regler samt god praxis

Vår genomlysning av Vårdgivaren visar att verksamheten saknar ett ledningssystem för informationssäkerhet, men kompenserar delvis för detta genom förekomsten av ett ledningssystem för GDPR. Det är dock vår bedömning att vissa områden av vikt för hantering av informationssäkerheten inte är tillräckligt utvecklade och formaliserade, däribland arbetet med kontroller hänförliga till åtkomst och förändringshantering, för att säkerställa att kraven på informationssäkerhet enligt Socialstyrelsens föreskrifter och allmänna råd, HSLF-FS 2016:40 (”Socialstyrelsens föreskrifter”), är uppfyllda.

Vidare noterar vi att Vårdgivaren har rutiner för att utvärdera sina leverantörer, men att de mallar som tillämpas inte är fullt anpassade för inköp av vårdtjänster. Därutöver har vi noterat att någon utvärdering av underleverantören MediCall inte har funnits att tillgå, vilket sammantaget indikerar att det föreligger svagheter vad gäller den interna kontrollen över leverantörsrelationer.

Vårdgivaren har sedan incidenten upprättat en åtgärdslista vilken bland annat innefattar en översyn av leverantörsbedömningar med fokus på informationssäkerhet, lösningar för realtidsövervakning av internetexponerade tillgångar hos såväl Vårdgivaren som dess underleverantörer, genomlysning och uppdatering av incidentprocesser samt genomförandet av ett projekt för certifiering inom ISO 27001. Vi noterar att vissa av åtgärderna beslutades innan incidenten. Vi har i samband med detta erhållit en väsentlig mängd styrkande dokument, varav flertalet är daterade maj 2019, men har inte haft möjligheten att inom ramen för detta uppdrag utvärdera och bedöma kvaliteten i dessa samt följa upp och testa i vilken mån de tillämpas. Vi rekommenderar HSF att följa upp Vårdgivarens arbete med införandet av ett ledningssystem för informationssäkerhet.

3. Iakttagelser och rekommendationer

Ref. nr.	Bed.	Iakttagelse	Risk för verksamheten	Rekommendationer
1	**HSF:s kravställning i avtalsprocessen**			
1.1	*Hög prio* 	**HSF saknar ett fullständigt ledningssystem för informationssäkerhet (LIS).** Enligt den regionsövergripande informationssäkerhetspolicyn ska varje nämnd införa ett lokalt ledningssystem för informationssäkerhet. I förekommande fall har HSF tagit fram lokala styrande dokument för informationssäkerhet, men dessa återspeglar i allt väsentligt de styrdokument som finns på regional nivå. Graden av verksamhetsanpassning är relativt låg och förvaltningen har inte tagit fram några instruktioner eller utvecklat processer för hanteringen av informationssäkerhet. Vi noterar att instruktioner håller på att arbetas fram, men dessa berör hanteringen av portabel IT-utrustning och syftar således inte till att tydliggöra riktlinjerna för hur förvaltningen ska arbeta med informationssäkerhet.	Bristande eller inkomplett LIS medför en väsentlig risk för att verksamheten inte kan säkerställa något enhetligt eller betryggande arbete vad gäller hanteringen av känslig information. Enligt vår bedömning försvårar detta även möjligheten att uppnå effektiva processer och ställa ändamålsenliga krav i avtalsprocessen.	Vi rekommenderar HSF att skyndsamt arbeta mot att införa ett komplett ledningssystem för informationssäkerhet, genom att: • Verksamhetsanpassa de styrande dokumenten. • Utarbeta instruktioner som tydliggör det löpande arbetet gällande informationssäkerhet, roller och ansvar samt sättet till vilket de olika rollerna/delarna av verksamheten samarbetar inom relevanta processer. • Tillse att principerna och arbetssätten kring informationssäkerhet implementeras i HSF:s ledningsprocesser.

1.2	*Hög prio* 	**HSF ställer inte tillräckligt tydliga krav på sina privata vårdgivare vad gäller deras informationssäkerhet.** Kravställningen på informationssäkerhet sker genom tillämpningen av en standardbilaga, vilken anger att leverantörer/vårdgivare ska följa regionövergripande styrande dokument för informationssäkerhet. Vi noterar att de styrande dokumenten, i sin tur, anger att informationssäkerheten hos de som arbetar på uppdrag av Region Stockholm ska regleras genom avtal. Vår bedömning är att dessa hänvisningar kan ge upphov till skiljande uppfattningar gällande kravbilden på informationssäkerheten. Med hänsyn till att Socialstyrelsen anger som krav att vissa kontrollmål ska uppfyllas beträffande informationssäkerheten, företrädesvis med stöd av ett LIS enligt standarder i ISO 27000-serien, är det även vår bedömning att HSF:s tillkommande avtalskrav endast ger en begränsad effekt vad gäller att tydliggöra förväntningarna på de privata vårdgivarna. Vi har i anslutning till vår granskning även kunnat konstatera att Vårdgivaren inte har något dokumenterat LIS och vi har inte heller kunnat identifiera att denna parameter har värderats inför den förnyade upphandlingen. Med utgångspunkt i vikten av en säker informationshantering bör HSF inte bara ha kontroller för att säkerställa förekomsten av ett LIS hos potentiella leverantörer, men även mekanismer för att avgöra hur brister i uppfyllelsen av avtalskrav gällande informationssäkerhet påverkar möjligheten till eventuella tilldelningar.	För otydliga avtalskrav medför hög risk för att leverantörer inte tolkar och applicerar kraven på ett betryggande sätt för HSF. Detta kan även bidra med svårigheter för avtalshandläggare att tolka avtalskraven samt försämrar förmågan att göra bedömningar kring graden av avtalsefterlevnad. Att inte följa upp denna Vårdgivarens efterlevnad av kravet om LIS kan, mot ljuset av den inträffade incidenten, innebära en risk mot anseendet för HSF i de fall allmänheten inte skulle uppfattat de vidtagna åtgärderna som tillräckliga.	Vi rekommenderar HSF att inleda ett arbete med att kategorisera sina leverantörer enligt portföljprincipen i syfte att bättre kunna prioritera resurser samt förtydliga kraven på strategiska leverantörer. Vi rekommenderar HSF att inkludera LIS, enligt standarden ISO 27001, som ett kvalificeringskrav i upphandlingar med strategiska leverantörer. Vi rekommenderar vidare HSF att systematiskt använda avtalsbilagorna för informationssäkerhet enligt den regionövergripande vägledningen ”Säkerställande av informationssäkerhet vid upphandling och avrop” (LS 2018-068). Detta bör göras med stöd av informationssäkerhetsklassificering kombinerat med de IT-säkerhetskrav som HSF redan tillämpar. Vi rekommenderar HSF att följa upp Vårdgivarens införande av ett LIS, enligt rekommendationerna under iakttagelse 3.1.
1.3	*Medel prio* 	**HSF saknar ändamålsenliga rutiner för att godkänna underleverantörer under pågående avtalsperiod.** Begäran om godkännande av underleverantörer som sker under pågående avtalsperiod hanteras av den enhet inom HSF som förvaltar det givna avtalet. Stickprov av godkännanden visar att	Att inte tillämpa en standardiserad process för godkännande av underleverantörer ökar risker kopplade till personberoende, där utformningen av underlagen samt tolkningen av de inkommande svaren kan innebära att	Vi rekommenderar HSF att införa ett standardiserat formulär för godkännande av underleverantörer vilket, baserat på tjänstens art och väsentlighet, bör ge en heltäckande beskrivning av underleverantörens förmåga till att leverera enligt förväntat.

		underlagen varierar i form och omfattning, där godkännanden i vissa fall har fattats utifrån begränsad information. Vi noterar exempelvis att underleverantörer har godkänts med ett tidigare godkännande som enda motivering. Då regelverk ständigt förändras och tilltar, samtidigt som ett företags ställning kan förändras vid varje given tidpunkt, är det vår bedömning att varje godkännande bör följa en strukturerad process för att säkerställa att inga väsentliga kriterier har förbisetts.	underleverantören inte utvärderas på ett heltäckande sätt.	Detta bör tillkomma med rutin för eskalering där expertkompetens kan rådfrågas beroende på de svar och underlag som lämnas in.
1.4	*Medel prio*	**Roller och ansvar samt antalet befintliga stödresurser inom informationssäkerhet är inte optimal med avseende på verksamhetens omfattning och art.** HSF:s arbete med informationssäkerhet utgår från ett antal roller vilka, utöver informationssäkerhetssamordnaren, bland annat innefattar informationssäkerhetsansvarig och informationssäkerhetskoordinatorer. I förekommande fall har vi förstått att den ansvarige utgörs av Hälso- och sjukvårdsdirektören, medan rollen som koordinator innehas av respektive avdelningschef med ansvar för att bidra i införandet av ett lokalt LIS. Med tanke på behovet av ämneskompetens, tillika koordinatorernas möjlighet att delta i det praktiska arbetet med att införa och förvalta ett LIS, är det vår bedömning att stödresurserna inom informationssäkerhetsområdet behöver stärkas. Detta är särskilt viktigt för att säkerställa ett ändamålsenligt gränssnitt mellan informationssäkerhetssamordnaren och de ansvariga för informationssäkerheten samt tillse att frågor kring kravställning och uppföljning hanteras tillfredsställande beaktat den mängd avtal som förvaltas inom HSF.	Att tillämpa en rollstruktur med begränsad kapacitet att införa och förvalta ett LIS medför risk för att informationssäkerheten hanteras av för få stödresurser, med för breda ansvarsområden. Detta kan i sin tur leda till att kritiska frågor inte hanteras på ett effektivt sätt.	Vi rekommenderar HSF att förstärka stödresurserna inom informationssäkerhetsområdet, med uppgift att agera stöd i avtals- och uppföljningsfrågor.

2.	Löpande uppföljning av vårdavtal			
2.1	*Hög prio* 	**HSF följer inte upp icke funktionella krav på ett strukturerat sätt.** HSF:s kravställning utgår från det givna vårdavtalet, standardiserade bilagor samt allmänna villkor. Vi kan i sammanhanget konstatera att HSF utför en ändamålsenlig uppföljning av kvaliteten i tjänsten baserat på själva vårdavtalet. Vi noterar samtidigt att uppföljningen inte följer en förutbestämd process, utan att avtalshandläggarna baserar uppföljningen på konkreta och mätbara villkor i avtalen samt utformar annan uppföljning med utgångspunkt i kunskap och preferens. I fråga om allmänna villkor och de standardiserade bilagorna är flertalet krav, däribland de om informationssäkerhet, allmänt hållna vilket ställer höga tolkningskrav på avtalshandläggarna. Vi kan konstatera att viss uppföljning har gjorts, däribland införandet av GDPR-rutiner hos Vårdgivaren, men det är samtidigt vår bedömning att någon heltäckande uppföljning inte har genomförts. Därutöver har vi noterat att Vårdgivaren enligt avtal ska upprätta och underhålla en incidentberedskap och kontinuitetsplan samt årligen revidera och presentera denna för HSF. Vi noterar att någon sådan inte har upprättats av Vårdgivaren, utan att man utgår från en plan som utarbetats med en annan vårdgivare.	Att avtalshandläggare ges ett för stort tolkningsansvar i förhållande till vissa typer av avtalskrav medför en ökad risk för brister i kritiska avtalsreglerade leveranser.	Vi rekommenderar HSF att utöka kravställningen mot strategiska leverantörer i enlighet med rekommendationerna under iakttagelse 1.2. Vi rekommenderar HSF att strukturera och standardisera processen för uppföljning samt i förväg bestämma vilka villkor som ska följas upp och på vilket sätt. I frågan om informationssäkerhet rekommenderar vi HSF att utforma kontroller för att säkerställa förekomsten av LIS hos strategiska leverantörer samt eskaleringsrutiner för genomförandet av eventuella platsbesök, med stöd av verksamhetens stödresurser. HSF bör även utforma frågebatterier som utgår från de kravkataloger som tagits fram inom ramen för Region Stockholms complianceprocess för informationssäkerhet.

3.	**Vårdgivarens efterlevnad av avtalsvillkor, lagar och regler samt god praxis**			
3.1	*Hög prio* 	**Vårdgivaren har inte tillräckliga processer för att säkerställa uppfyllandet av Socialstyrelsens krav på informationssäkerhet.** Processer och rutiner ska finnas för att säkerställa uppfyllandet av Socialstyrelsens krav på informationssäkerhet. Vårdgivaren har inget dokumenterat LIS och det är vår bedömning att vissa processer saknas för att kunna försäkra att kraven uppfylls. Vi noterar exempelvis att Vårdgivaren, i enlighet med vedertagna standarder och god praxis, inte har ställt ändamålsenliga krav på samt följt upp leverantörers hantering av informationssäkerhet. Vidare anger Socialstyrelsen att vårdgivare ska ha en informationssäkerhetspolicy som anger mål och inriktning på verksamhetens arbete med informationssäkerhet. Vi har identifierat att Vårdgivaren har antagit en informationssäkerhetspolicy i maj 2019. Vi noterar i sammanhanget att Vårdgivaren planerar för en certifiering inom ISO 27001 till kvartal 2, 2020 samt har ett ledningssystem för GDPR.	Ofullständiga processer beträffande arbetet med informationssäkerhet medför risk för att verksamheten inte förmår att hantera känslig information på ett ändamålsenligt och betryggande sätt.	Vi rekommenderar Vårdgivaren att skyndsamt införa ett LIS i enlighet med utarbetad åtgärdsplan. Vi rekommenderar Vårdgivaren att genomföra en fördjupad utvärdering av mognadsgraden inom informationssäkerhet samt kommunicera resultatet till HSF. Vi rekommenderar HSF att följa upp Vårdgivarens arbete med införandet av ett LIS samt säkerställa att slutförandet sker under andra kvartalet 2020, i enlighet med Vårdgivarens egen tidplan.
3.2	*Medel prio* 	**Bristande kontroller hänförliga till åtkomst och förändringshantering hos underleverantörer till vårdtjänsten.** Enligt Vårdgivaren beror incidenten på en felkonfigurerad lagringsenhet i samband med uppgraderingen av underleverantören MediCalls utkontrakterade IT-plattform. Vi noterar att förekomsten av ett fullständigt LIS hade adresserat frågan genom dedikerade processer för kravställning och uppföljning av tredje part.	Brister i kontroller för åtkomst och förändringshantering ökar väsentligen risken för otillbörlig åtkomst av känslig information.	Vi rekommenderar Vårdgivaren att skyndsamt aktualisera relevanta rutiner samt tillse att motsvarande rutiner implementeras hos verksamhetskritiska leverantörer.
3.3	*Medel prio* 	**Vårdgivarens kontroll av leverantörer är inte fullt anpassad till vårdverksamhet.** Vårdgivaren har mallar för bedömning av leverantörer, men dessa är riktade mot inköp av varor med fokus på kvalitetsaspekter. Vår bedömning är att dessa, i dagsläget, inte är anpassade till att	Otillräcklig kontroll av leverantörer medför en väsentlig risk för såväl Vårdgivaren som HSF vad gäller förmågan att kunna leverera vårdtjänsten på ett	Vi rekommenderar Vårdgivaren att vidareutveckla processer och mallar för utvärdering av leverantörer i frågor som rör informationssäkerhet. Detta innefattar att vidareförmedla de

		bedöma leverantörer i samband med inköp och upphandling av vårdtjänster. Vi noterar dock att Vårdgivaren, redan innan incidenten, har arbetat med att uppdatera och förbättra utvärderingsunderlagen. Vår genomlysning har även visat att något utvärderingsunderlag inte funnits att tillgå för leverantören i fråga, vilket tyder på förekomsten av kontrollbrister i processen för inköp.	tillfredsställande sätt. Att Vårdgivaren brister i kontrollen av sina leverantörer ökar även risken för att HSF inte förmår att ta informerade beslut kring godkännandet av potentiella underleverantörer.	avtalskrav som framställs i det underliggande vårdavtalet, i de fall leverantören agerar underleverantör till HSF avseende vårdtjänster. Vi rekommenderar Vårdgivaren att tillse att internkontrollsystemet är ändamålsenligt och effektivt för att säkerställa att processer och rutiner efterlevs på ett tillfredsställande sätt. Vi rekommenderar HSF att stärka sin process för godkännande av underleverantörer, se rekommendation under iakttagelse 1.3.

4. Bilagor

4.1 Bilaga 1: Kriterier för utvärdering

Den sammanfattande bedömningen av effektivitet och ändamålsenlighet i den interna styrningen och kontrollen avseende enskilda iakttagelser i granskningen klassificeras i tre nivåer enligt nedan.

Klassificering av enskilda iakttagelser i granskningen	
Låg prioritet	Iakttagelsen bedöms troligen inte kunna resultera i finansiella eller operationella förluster men kan inrymma möjligheter att förbättra effektivitet och ändamålsenlighet. Korrigerande åtgärder rekommenderas.
Medelprioritet	Iakttagelsen är av återkommande karaktär eller bedöms kunna resultera i finansiella eller operationella förluster om inga åtgärder vidtas. Korrigerande åtgärder bör hanteras inom rimlig tidsperiod.
Hög prioritet	Iakttagelsen kan på kort tid resultera i finansiell eller operationell förlust inom området om den inte åtgärdas. Rekommenderar att åtgärd snarast implementeras.

4.2 Bilaga 2: Intervjuade personer

Hälso- och sjukvårdsförvaltningen

- Carina Landberg, Enhetschef, Strategisk informationshantering
- Carl Mill, Strateg, Verksamhetsplanering och uppföljning
- Charlotte Falk Johansson, Verksamhetsutvecklare, Verksamhetsplanering och uppföljning
- Dan Billtorp, Dataskyddsombud, Styrning och ekonomi
- Jenny Oldsjö, Inköpsstrateg, Administrativa avdelningen
- Kristin Blixt, Handläggare, Styrning och ekonomi
- Lenah Hedberg, IT-utredare/Dataskyddsombud, Styrning och ekonomi
- Lena Franzén Byttner, Handläggare, Strategisk planering
- Lena Furmark, Avdelningschef
- Lisa Hagberg, Enhetschef, Verksamhetsplanering och uppföljning
- Melisa Flodman, Informationssäkerhetssamordnare, Strategisk informationshantering
- Richard Broddvall, Enhetschef, Strategisk planering
- Stefan Pettersson, Avtalshandläggare 1177 VPT, Verksamhetsplanering och uppföljning

Regionledningskontoret

- Claudia Bush Bäckman, Upphandlare
- Josef Driving, Jurist
- Stefan Schildt, IT-direktör
- Vesna Lucassi, Informationssäkerhetschef

MedHelp AB

- Björn Arkinger, Affärsområdeschef Vårdtjänster
- Daniel Seid, Dataskyddsombud, konsult Triage SEC AB
- Peter Wallin, Chief Technology Officer