Hälso- och sjukvårdsförvaltningen

TJÄNSTEUTLÅTANDE
2016-03-03

HSN 1506-0806

Handläggare:
Bill Heiding, Carina Landberg

Hälso- och sjukvårdsnämnden
2016-04-19, p 11

Lokal informationssäkerhetspolicy för hälso- och sjukvårdsförvaltningen

Ärendebeskrivning

I Stockholm läns landsting fastställda policy och riktlinjer för informationssäkerhet finns i uppdrag att hälso- och sjukvårdsnämnden ska upprätta en lokal informationssäkerhetspolicy.
hälso- och sjukvårdsförvaltningen har tagit fram ett förslag till lokal policy för informationssäkerhet i syfte att säkerställa ett strukturerat och långsiktigt arbete inom området.
Hälso- och sjukvårdsnämnden föreslås anta föreslagen lokal informationssäkerhetspolicy för Hälso- och sjukvårdsförvaltningen.

Beslutsunderlag

Hälso- och sjukvårdsdirektörens tjänsteutlåtande, 2016-03-03
Lokal informationssäkerhetspolicy för hälso- och sjukvårdsförvaltningen

Förslag till beslut

Hälso- och sjukvårdsnämnden beslutar

att anta föreslagen informationssäkerhetspolicy - Lokal informationssäkerhetspolicy för hälso- och sjukvårdsförvaltningen

att uppdra åt hälso- och sjukvårdsdirektören att fastställa framtida ändringar och tillägg till lokal informationssäkerhetspolicy

att uppdra åt hälso- och sjukvårdsdirektören att upprätta och fastställa informationssäkerhetsriktlinjer för hälso- och sjukvårdsförvaltningen

att uppdra åt hälso- och sjukvårdsdirektören att upprätta och fastställa handlingsplan för informationssäkerhet

att uppdra åt hälso- och sjukvårdsdirektören att vid behov utarbeta lokala anvisningar och instruktioner inom informationssäkerhetsområdet.

Förvaltningens motivering till förslaget

Fullmäktige i Stockholms läns landsting (SLL) fattade den 19 mars 2013 beslut kring en policy och riktlinjer för informationssäkerhet (LS1112-1733). Dessa utgör stommen i det ledningssystem för informationssäkerhet som ska gälla inom SLL. Som ett led i detta arbete har varje förvaltning till uppgift att implementera ledningssystem för informationssäkerhet.

Hälso- och sjukvårdsförvaltningens direktör fattade den 29 juni 2015 beslut kring införandet av Ledningssystem för informationssäkerhet (LIS) i syfte att öka informationssäkerheten på hälso- och sjukvårdsförvaltningen (HSN1401-0002). Som ett led i detta arbete ska hälso- och sjukvårdsnämnden fastställa lokal policy för informationssäkerhet.

Den lokala informationssäkerhetspolicyn för hälso- och sjukvårdsförvaltningen är identisk med Stockholms läns landstings policy och riktlinjer för informationssäkerhet, med undantag för anpassningar till hälso- och sjukvårdsförvaltningens uppdrag.

Stockholms läns landsting står inför en stor förändringsprocess. För att möta framtidens behov genomför landstinget just nu en av de största satsningarna någonsin inom hälsa och vård. Genomförandet av framtidsplanen kräver en hög förändringstakt, vilket i sin tur kommer att ställa högre krav på informationshantering och informationssäkerhet inom landstinget. Samtidigt ställer en stark utveckling av informationssäkerhetsfrågorna i samhället, i allmänhet, ökade krav på landstingets förmåga inom området.

Syftet med förslaget är att skapa förutsättningar för att bedriva ett systematiskt informationssäkerhetsarbete inom Hälso- och sjukvårdsförvaltningen, och etablera nödvändiga stödstrukturer för informationssäkerhet på verksamhetsnivå. Fokus ligger på att skapa en struktur för ledning och styrning på både övergripande och lokal nivå, d.v.s. verksamhetsnivå, och därigenom skapa förutsättningar för att hålla informationssäkerhetsarbetet levande och målen i policyn tydliga.

Att upprätta verksamhetsnära ledningssystem är ett ändamålsenligt sätt att långsiktigt hantera och utveckla hälso- och sjukvårdsförvaltningens informationssäkerhetsarbete. I Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården, SOSFS 2008:14, anges att en vårdgivare ska ha en dokumenterad informationssäkerhetspolicy som gör att patientuppgifter hanteras på ett säkert sätt i verksamheten. I det föreslagna regelverket för informationssäkerhet motsvarar detta den lokala informationssäkerhetspolicyn.

Den lokala policyn har arbetats fram i samråd med landstingets informationssäkerhets chef och representanter från förvaltningen. Uppföljning görs årligen av efterlevnaden av informationssäkerhetsarbetet.

Genom föreslagen lokal policy höjs ambitionsnivån för informationssäkerhetsarbetet inom hälso- och sjukvårdsförvaltningen.

Förtydligande avseende uppdraget till förvaltningsdirektören att besluta om ändringar och tillägg
Med hänsyn till att policy, riktlinjerna, anvisningar och instruktioner kan behöva revideras och uppdateras i enlighet med till exempel förändringar i författningskrav föreslås hälso- och sjukvårdsnämnden delegera viss beslutskompetens till förvaltningsdirektören som bemyndigas att i sin tur vidaredelegera beslutanderätten till någon annan anställd. Avsikten är att genomföra justeringar i policy, riktlinjer, anvisningar och instruktioner som kan anses vara av mindre karaktär och syfta till att förtydliga eller anpassa dessa till förändrade förutsättningar.

Ekonomiska konsekvenser
Det uppstår inga ekonomiska konsekvenser av beslutet. Kostnaderna för ovan beskrivna aktiviteter ryms inom ordinarie budget. Kostnaderna för genomförandet ska rymmas inom respektive verksamhets budget. Innehållet i lokala riktlinjer och handlingsplanen motsvarar till största del krav som redan ställs på landstingets verksamheter liksom redan beslutade åtgärder.

Konsekvenser för patientsäkerhet
En korrekt informationshantering och systematiskt informationssäkerhetsarbete ökar patientsäkerheten och skyddar individen.

Konsekvenser för jämställd och jämlik vård
Informationssäkerhetsarbetet i sig har ingen påverkan på jämställd och jämlik vård.

Miljökonsekvenser
Beslutet får oförändrade konsekvenser för miljön.

Barbro Naroskyin
Hälso- och sjukvårdsdirektör

Lena Furmark
Avdelningschef

Lokal informationssäkerhetspolicy för

Hälso- och sjukvårdsförvaltningen

Hälso- och sjukvårdsförvaltningen
08-123 132 00
Datum: 2016-03-03
Diarienummer: HSN1506-0806

Hälso- och sjukvårdsförvaltningen
STOCKHOLMS LÄNS LANDSTING

Innehållsförteckning

Ver	Datum	Förändring	Ändrat av
0.1	2015-09-29	Utkast upprättat	Informationssäkerhetssamordnare, Bill Heiding
0.2	2015-10-08	Granskat och uppdaterat	IT-arkitekt, säkerhet, Lars-Erik Hillberg
0.3	2015-10-13	Granskat och uppdaterat	Enhetschef, Christina Sollenberg
0.4	2016-01-08	Mindre justeringar	Informationssäkerhetssamordnare, Bill Heiding
0.5	2016-01-18	Uppdaterat roller och ansvar	Justeringar efter presentation för LGIT
0.6	2016-03-03	Granskad och uppdaterad	Tf Enhetschef Carina Landberg

1 Inledning

1.1 Övergripande Stockholms läns landsting

Stockholms läns landstings verksamhet är grundad på principer om öppenhet, personlig integritet och respekt för individen. Medborgarna ska kunna få insyn i landstingets verksamhet. De ska kunna förlita sig på den information som landstinget lämnar och vara förvissade om att information som samlas in får ett tillräckligt skydd.

Information är en av landstingets mest strategiska resurser. Alla verksamheter är beroende av tillförlitlig information. Avbrott i tillgången till information kan vara kritiskt och felaktig information kan ge allvarliga konsekvenser inom hälso- och sjukvården, kollektivtrafiken och inom landstingets övriga ansvarsområden.

Utvecklingen med informationshantering i IT-system och nya funktionaliteter innebär förbättringar i många avseenden. Samtidigt innebär beroendet av informationssystem att sårbarheten och riskexponeringen ökar om inte säkerhetsaspekterna beaktas.

Därför arbetar Stockholms läns landsting aktivt med informationssäkerhet. Det innebär att se till att informationstillgångar finns tillgängliga när de behövs, att de är korrekta, och att obehöriga inte får åtkomst till dem. Genom att arbeta systematiskt och långsiktigt upprätthåller vi ett tillräckligt skydd som är anpassat efter våra verksamheters förutsättningar och behov.

Informationssäkerhetsarbetet syftar till att stödja och säkerställa landstingets verksamhet. Alla medarbetare deltar i detta arbete. Informationssäkerhetsarbetet är en viktig del i landstingets övergripande arbete med intern styrning och kontroll samt riskhantering.

1.2 Hälso-och sjukvårdsförvaltningen

Varje nämnd, styrelse och bolag i Stockholms läns landsting skall ha en egen lokal informationssäkerhetspolicy för dess verksamhetsområde.

Denna policy är den lokala policyn för Hälso- och sjukvårdsförvaltningen (HSF). Den är identisk med Stockholms läns landstings policy för informationssäkerhet, med undantag för anpassningar till Hälso- och sjukvårdsförvaltningen.

Policyn behandlar informationssäkerheten för HSF:s interna verksamhet. Den beskriver de övergripande principer som ska gälla för informationssäkerhetsarbetet på Hälso- och sjukvårdsförvaltningen.

2 Mål

Målet för Hälso- och sjukvårdsförvaltningen informationssäkerhetsarbete är att skydda informationen inom verksamheten. Skyddet ska vara anpassat till skyddsvärde, risk och lagkrav och därigenom möjliggöra för förvaltningens verksamheter att uppnå sina mål.

En god informationssäkerhet inom Hälso- och sjukvårdsförvaltningen främjar verksamheternas funktionalitet, kvalitet och effektivitet, medborgares rättigheter och personliga integritet, Hälso- och sjukvårdsförvaltningens förmåga att förebygga och hantera allvarliga störningar och kriser samt förtroendet för förvaltningens informationshantering samt IT-system.

3 Omfattning

Informationssäkerhetspolicyn gäller för hantering av information, i alla dess former, i Hälso- och sjukvårdsförvaltningen och av samtliga som arbetar på uppdrag av förvaltningen. Det sistnämnda regleras genom avtal.

Informationssäkerhetsarbetet styrs med hjälp av landstingets ledningssystem för informationssäkerhet som är framtaget med stöd av standarden för informationssäkerhet, ISO/IEC 27000 och utifrån organisationens verksamhetskrav samt gällande lagar och föreskrifter.

HSF:s ledningssystem är uppbyggt i två nivåer. Nivåerna ger en struktur för ledning och styrning av informationssäkerheten på både övergripande nivå och på verksamhetsnivå. En viktig del av ledningssystemet är regelverket. Det består av styrande dokument som på förvaltningsnivå utgörs av denna policy och tillhörande riktlinjer och anvisningar. Allt informationssäkerhetsarbete utgår från dessa dokument.

Hälso- och sjukvårdsnämnden styr informationssäkerhetsarbetet i ett lokalt ledningssystem inom sitt verksamhetsområde. Det innehåller de nödvändiga processer och rutiner som behövs för att säkerställa att verksamheten uppfyller kraven på en ändamålsenlig informationssäkerhet. De styrande dokumenten på lokal nivå utformas utifrån de landstingsövergripande.

Utöver detta krävs att Hälso- och sjukvårdsförvaltningen i tillämpliga delar lever upp till gällande lagar och förordningar samt till förvaltningens övriga styrande dokument.

4 Innebörd

Informationssäkerhetsarbetet innebär att värdera all information efter sin känslighet och med hjälp av administrativa och tekniska skyddsåtgärder säkerställa att den finns

tillgänglig när den behövs, att den är korrekt och att obehöriga inte kan få tillgång till den. Utöver dessa säkerhetsaspekter måste behov av spårbarhet uppfyllas - att i efterhand kunna avgöra vem som tagit del av informationen, vilka förändringar som skett och av vem dessa utförts.

4.1 Säkerhetsaspekter

Konfidentialitet (rätt person):	Information får inte göras tillgänglig eller avslöjas på ett sådant sätt att den personliga integriteten eller sekretessen hotas.
Riktighet (rätt information):	Informationen få inte förändras eller gå förlorad, av misstag, genom inverkan av obehörig eller på grund av tekniskt fel.
Tillgänglighet (rätt tid och plats):	Informationen ska kunna användas i förväntad utsträckning, inom önskad tid och på rätt plats.
Spårbarhet:	Händelser i informationsbehandlingen ska kunna spåras.

Skyddet av informationstillgångar och informationssystem ska vara utformat så att verksamhetens krav på dessa säkerhetsaspekter uppfylls. Detta gäller även när Hälso- och sjukvårdsförvaltningens information eller informationssystem hanteras av extern part.

4.2 Skyddsåtgärder

För att hitta relevant skyddsnivå utifrån dessa fyra aspekter ska HSF arbeta utifrån nedanstående principer:

- HSF ska arbeta med informationsklassificering där information klassificeras och handlingar och dokument märks.
- All information ska ha en ägare. Informationsägaren ansvarar för att klassificera informationen och ställa de säkerhetskrav som krävs för informationshantering.
- Alla informationssystem ska ha en systemägare som ansvarar för att säkerhetskraven på systemet uppfylls.
- Omvärlden förändras. Därför ska HSF, utifrån återkommande risk- och sårbarhetsanalyser och inträffade incidenter, vidta nödvändiga åtgärder för att se till att vår information har rätt skydd.
- HSF ska ställa säkerhetskrav inför upphandling, utveckling, användning och avveckling av informationssystem och vi ska följa upp de krav vi ställt.
- HSF ska arbeta med kontinuitetsplanering och ha beredskap för avbrott. Våra kritiska verksamheter ska kunna upprätthållas på fastställd nivå vid olika typer av katastrofsituationer, störningar och avbrott.

- Alla anställda ska veta vad det egna ansvaret omfattar och ha god kunskap om vilka säkerhetsregler som gäller. Detsamma gäller när tillfällig eller extern personal anlitas.
- Det är viktigt att alla har ett högt säkerhetsmedvetande och kritiskt ifrågasätter händelser som kan påverka informationssäkerheten.
- Skyddsåtgärder skall vara kostnadseffektiva och stå i proportion till värdet av informationen och de negativa konsekvenser en otillräcklig säkerhet kan medföra.
- Kontinuerlig uppföljning ska ske mot fastställda regler.

5 Ansvar

5.1 Övergripande Stockholm läns landsting

Landstingsfullmäktige fastställer den informationssäkerhetspolicy som ska gälla för landstinget.

Landstingsstyrelsen ansvarar för att landstingets informationssäkerhets policy och riktlinjer för informationssäkerheten utarbetas och hålls aktuella. Landstingsstyrelsen ansvarar också för samordningen av informationssäkerhetsarbetet i landstinget och ska därför årligen fastställa en övergripande handlingsplan för informationssäkerhetsarbetet.

Landstingsdirektören har landstingstingsstyrelsens uppdrag att sörja för att informationssäkerhetsarbetet bedrivs så effektivt som möjligt. Landstingsdirektören ansvarar för att övergripande tillämpningsanvisningar utarbetas och hålls aktuella i enlighet med policy och riktlinjer.

Informationssäkerhetschefen verkställer samordningen av informationssäkerhetsarbetet inom landstinget och förvaltar denna policy, de tillhörande riktlinjerna och tillämpningsanvisningarna samt den övergripande handlingsplanen för informationssäkerhet.

Varje nämnd och styrelse är ansvarig för informationssäkerheten inom sitt verksamhetsområde och ska därför, inom ramen för sitt lokala ledningssystem och i enlighet med tillämpningsanvisningar, anta verksamhetsnära styrdokument för informationssäkerhet. För HSNs del är det denna policy som avses. Det åligger även varje nämnd och styrelse att årligen planlägga och löpande följa upp informationssäkerheten och i övrigt vidta de åtgärder som krävs för att uppnå och upprätthålla tillräcklig intern kontroll.

Förvaltningschef/VD ska säkerställa att all informationshantering inom den egna verksamheten sker i enlighet med denna policy samt tillhörande riktlinjer och tillämpningsanvisningar för informationssäkerhet.

Informationssäkerhetssamordnare ska utses inom varje förvaltning och bolag och ges i ansvar att samordna och följa upp det för organisationen och verksamheten gemensamma informationssäkerhetsarbetet.

Varje anställd ansvarar för att uppställda säkerhetsregler följs samt att störningar och fel i informationssystem, utrustningar och informationsinnehåll rapporteras enligt fastställda rutiner.

SLL:s informationssäkerhetsråd uppgift är att främja, stödja, samordna och följa upp landstingets informationssäkerhetsarbete på en övergripande nivå.

Landstingsrevisorernas uppgift är att granska om den interna kontrollen är tillräcklig.

5.2 Hälso- och sjukvårdsförvaltningen

Hälso- och sjukvårdsförvaltningen har ett gemensamt ledningssystem för informationssäkerhet, LIS. Det ägs av Hälso-och sjukvårdsdirektören, och förvaltas av förvaltningens informationssäkerhetssamordnare. Ledningssystemet består av denna policy, riktlinjer och instruktioner. Riktlinjerna är identiska med de riktlinjer som är utgivna för Stockholms läns landsting som helhet. Instruktionerna är lokala för Hälso- och sjukvårdsförvaltningen. En instruktion kan undantagsvis vara lokal för en eller flera avdelningar inom Hälso- och sjukvårdsförvaltningen oftast är den en lokal anpassning av landstingets tillämpningsanvisningar.

Hälso- och sjukvårdsförvaltningen ska ha en utsedd informationssäkerhetssamordnare som koordinerar arbetet.

Avdelnings chefer ansvarar för informationssäkerheten inom respektive verksamhet och uppföljning av informationssäkerhet till informationssäkerhetssamordnaren.

Informationssäkerhetssamordnaren skall årligen sammanställa en informationssäkerhetsrapport, som redogör för väsentliga risker, avvikelser, informationssäkerhets incidenter och förslag till prioriterat arbete. Informationssäkerhetssamordnaren skall ha regelbundna avstämningar med förvaltningens personuppgiftsombud, med informationssäkerhetskontakter i verksamheten och ansvarar för att representera Hälso- och sjukvårdsförvaltningen i Stockholms läns landstings informationssäkerhetsråd (ISR) samt vara Hälso- och sjukvårdsförvaltningens kontaktperson gentemot landstingets informationssäkerhetschef. Informationssäkerhetssamordnaren ska rapportera regelbundet i Hälso- och sjukvårdsförvaltningen ledningsgrupp.

6 Drift och systemförvaltning

6.1 Drift, systemförvaltning av extern part

När Hälso- och sjukvårdsförvaltningen lägger ut datordrift, systemförvaltning eller bearbetning av information till en annan part, skall den externa parten förbinda sig att minst årligen rapportera om genomförd egenkontroll av informationssäkerheten och eventuella avvikelser. När leverantören är en extern part, har respektive avdelningschef

inom Hälso- och sjukvårdsförvaltningen ansvaret för att uppdraget utförs i enlighet med gällande lagstiftning, policys och riktlinjer. Avdelningschefen är ansvarig för att regelbunden rapportering av sådana externa samarbeten, och dess årliga uppföljningar av informationssäkerhetens efterlevnad och eventuella avvikelser. Rapportering sker till informationssäkerhetssamordnare och även i förekommande fall till personuppgiftsombud.

6.2 Drift, systemförvaltning av SLL-IT

När leverantören är en del av Stockholms läns landsting, t.ex. SLL IT, omfattas den av landstingets övergripande policy och riktlinjer. När underleverantörer används har leverantören ansvar för att underleverantör också följer landstingets övergripande policy och riktlinjer. Leverantören ska regelbundet göra uppföljning av underleverantörens informationssäkerhets efterlevnad. Hälso- och sjukvårdsförvaltningen som kund förväntas inte behöva kontrollera efterlevnaden av dessa. En årlig rapport skall dock inges till Hälso- och sjukvårdsförvaltningens informationssäkerhetssamordnare av informationssäkerhets efterlevnaden och eventuella avvikelser.

6.3 Drift, systemförvaltning utförda av Hälso- och sjukvårdsförvaltningen

När Hälso- och sjukvårdsförvaltningen tar uppdrag om datordrift, systemförvaltning eller bearbetning av information från vårdgivare, annat landsting eller annan extern part, skall Hälso- och sjukvårdsförvaltningens ledningssystem för informationssäkerhet gälla, om det inte i överenskommelsen framgår vilket annat ledningssystem för informationssäkerhet som skall användas. Respektive avdelningschef på Hälso- och sjukvårdsförvaltningen har ansvaret för att uppdraget utförs i enlighet med gällande lagstiftning, policys och riktlinjer. Avdelningschefen är ansvarig för att årliga uppföljningar av informationssäkerheten och eventuella avvikelser sker till informationssäkerhetssamordnare. Det skall finnas tydligt informationsägarskap och avtalat Personuppgiftsansvarig (PUA)/ Personuppgiftsbiträde (PUB) ansvar.

7 Uppföljning och revidering

Uppföljning och revidering av denna policy ska ske regelbundet. I samband med revidering ska tillhörande riktlinjer och instruktioner samt handlingsplanen för informationssäkerhet revideras på motsvarande sätt.