Göteborgs Stad Örgryte-Härlanda
Box 17094
402 61 GÖTEBORG

Vårdgivare

Örgryte-Härlanda stadsdelsnämnd i Göteborgs stad.

Ärendet

Tillsyn av Örgryte-Härlanda stadsdelsnämnds systematiska informationssäkerhetsarbete i egenskap av leverantör av samhällsviktig tjänst inom hälso- och sjukvårdssektorn enligt NIS[1].

Beslut

Inspektionen för vård och omsorg (IVO) anser att Örgryte-Härlanda stadsdelsnämnd inte bedriver något systematiskt och riskbaserat informationssäkerhetsarbete. IVO har identifierat följande brister vid tidpunkten för inspektionen.

- Örgryte-Härlanda stadsdelsnämnd har inte genomfört någon övergripande riskanalys och hade inte någon plan för genomförandet av en övergripande riskanalys som ska utgöra grund för beslut om lämpliga säkerhetsåtgärder.
- Ledningens och övriga organisationens ansvar för det systematiska informationssäkerhetsarbetet är inte tydliggjort i tillräcklig omfattning.
- Örgryte-Härlanda stadsdelsnämnd bedriver inte informationssäkerhetsarbetet enligt internationella standarder.

IVO begär med stöd av 7 kap. 20 § patientsäkerhetslagen (2010:659) att nämnden redovisar sin inställning till de brister som IVO konstaterat. Redovisningen ska även innehålla de eventuella åtgärder som nämnden har vidtagit eller planerar att vidta för att komma till rätta med bristerna. Redovisningen ska avslutas med uppgift om när åtgärden genomfördes eller kommer att genomföras.

- Redovisningen ska ha kommit in till IVO senast den 15 april 2020.

[1] Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen.

IVO kan, om bristerna inte avhjälps, komma att fatta beslut om att förelägga nämnden att vidta åtgärder.

Skälen för beslutet

IVO:s granskning av har visat att Örgryte-Härlanda stadsdelsnämnd brister i det systematiska och riskbaserade informationssäkerhetsarbetet inom nedanstående granskade områden.

Stadsdelen genomför inte en årlig riskanalys på övergripande nivå.

IVO bedömer att Örgryte-Härlanda stadsdelsnämnd inte har genomfört en årlig, övergripande riskanalys avseende informationssäkerheten i nätverk och informationssystem.

Av 12 § lagen (2018:1174) om informationssäkerhet för leverantörer av samhällsviktiga tjänster, LIS, framgår att leverantören ska göra en riskanalys som ska ligga till grund för val av säkerhetsåtgärder. I riskanalysen ska det också ingå en åtgärdsplan. Analysen ska dokumenteras och uppdateras årligen.

Vid inspektionen framkom att stadsdelen främst har arbetat med riskanalys vid klassning av information. Stadsdelen har vid tidigare informationsklassning utgått från tillgänglighet och konfidentialitet men inte beaktat riktighet eller spårbarhet. Riskanalysen vid informationsklassningen har lett till en åtgärdsplan med nya rutiner som ska följas upp varje år.

Stadsdelen har dock inte gjort någon årlig sammanhållen riskanalys för informationssäkerhet på övergripande nivå. IVO bedömer därför att nämnden inte i tillräcklig omfattning genomför riskanalyser som ska ligga till grund för val av och beslut om lämpliga säkerhetsåtgärder.

Ledningens och organisationens ansvar för det systematiska informationssäkerhetsarbetet är inte tydliggjort

IVO bedömer att ledningen och övriga organisationens ansvar inte är tydliggjort i tillräcklig omfattning.

Vid inspektionen redogjorde stadsdelens representanter för att informationssäkerhetsansvaret följer linjeorganisationen. Nämnden har det yttersta ansvaret och arbetar på uppdrag av kommunfullmäktige.

Göteborgs stad är organiserad så att varje nämnd utgör en egen förvaltning, är en egen vårdgivare och således en leverantör av en samhällsviktig tjänst. På grund av stadens organisation ansåg stadsdelen att de inte ägde vissa informationssäkerhetsfrågor fullt ut. Det fanns inte heller någon sakkunnig eller stödfunktion på central nivå dit stadsdelen kunde vända sig med informationssäkerhetsfrågor.

IVO begärde vid tillsynen in vårdgivarens rutiner och riktlinjer för informationssäkerhetsarbetet i stadsdelen.

Det visade sig att det fanns en stadsövergripande "Säkerhetspolicy för Göteborgs Stad" samt en stadsövergripande "Riktlinje för informationssäkerhet", bägge daterade den 5 augusti 2013. Däremot saknades vid tidpunkten för inspektionen fastställd dokumentation som beskrev hur arbetet med informationssäkerhet skulle bedrivas i stadsdelen. IVO har tagit del av ett arbetsmaterial " SDF Örgryte-Härlandas Riktlinje för informationssäkerhet" men det dokumentet var inte fastställt.

IVO konstaterar att arbetet med att tydliggöra ledningens och övriga organisationens ansvar var påbörjat men att det fanns behov av ett fortsatt utvecklingsarbete för att leva upp till bestämmelserna i 6 § MSBFS 2018:8. Det framgår av bestämmelsen att en leverantör utifrån identifierade risker och behov bland annat ska tydliggöra ledningens och övriga organisationens ansvar avseende informationssäkerhetsarbetet. Leverantören ska också tilldela nödvändiga resurser, mandat och befogenheter för de funktioner som arbetar med informationssäkerhet samt säkerställa att informationssäkerhetsarbetet regelbundet och vid behov utvärderas och anpassas.

Stadsdelen bedriver inte informationssäkerhetsarbetet enligt internationella standarder för informationssäkerhet

IVO anser att stadsdelen inte kan påvisa att de vid tidpunkten för inspektionen bedrev informationssäkerhetsarbetet enligt ISO 27000-serien.

Vid tillsynen framkom att stadsdelen ser standarderna i ISO 27000-serien som riktlinjer och stadsdelen har inte för avsikt att certifiera sig mot en standard. Enligt stadsdelens representanter ska den övergripande riktlinjen i Göteborgs stad daterad 2013-08-05 vara upprättad utifrån standarder. IVO kan dock konstatera att det inte framkommer i riktlinjen vilka standarder som den grundar sig på. Vidare har ISO 27000-serien uppdaterats 2017 och riktlinjen är från 2013.

Av bestämmelserna i 5 § MSBFS 2018:8 framgår det bland annat att varje leverantör ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av standarderna SS-EN ISO/IEC 27001:2017 och SS-EN ISO/IEC 27002:2017 om ledningssystem för informationssäkerhet eller motsvarande. Det systematiska och riskbaserade informationssäkerhetsarbetet ska utformas och samordnas utifrån organisationens behov. Det ska vara styrande avseende informationshantering i nätverk och informationssystem som används för att tillhandahålla samhällsviktiga tjänster. Arbetet ska dokumenteras.

Övrigt

IVO har noterat att dokumentet "SDF Örgryte-Härlandas riktlinje för informationssäkerhet" enbart hänvisar till tre så kallade

lagbestämmelser, Dataskyddsförordningen (GDPR), LIS och förordningen (2018:1175) till LIS. IVO vill påtala att annan relevant författning är patientdatalagen (2008:355), HSLF-FS 2016:40, MSBFS 2018:8 och MSBFS 2018:9.

Underlag

- Protokoll från inspektionen den 21 november 2019
- Örgryte-Härlanda stadsdelsnämnds riktlinjer för informationssäkerhet
- Göteborg Stads "Säkerhetspolicy" samt "Riktlinjer för informationssäkerhet" daterade 2013-08-05.

Ytterligare information

IVO genomförde den 21 november 2019 en inspektion av stadsdelsnämnd Örgryte-Härlandas systematiska och riskbaserade informationssäkerhetsarbete. Tillsynen utgår från 11-14 §§ lagen om informationssäkerhet (2018:1174) för leverantörer av samhällsviktiga och digitala tjänster, LIS, samt Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2018:8) om informationssäkerhet för leverantörer av samhällsviktiga tjänster. Granskningen har skett utifrån kraven enligt ovanstående bestämmelser att tydliggöra ledningens och organisationens ansvar för informationssäkerhetsarbetet, genomföra riskanalyser och bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av standarderna SS-EN ISO/IEC 27001:2017 och SS-EN ISO 27002:2017. Informationssäkerhetsarbetet ska vara dokumenterat. Tillsynen sker med stöd av 24-25 §§ LIS.

Beslut i detta ärende har fattats av inspektören Anna Nordsjö. Inspektörerna Eva-Lena Pettersson och Krister Lundström har deltagit i den slutliga handläggningen. Inspektören Johanna Rydbäck har varit föredragande.

För Inspektionen för vård och omsorg

Anna Nordsjö

Johanna Rydbäck