Informationssäkerhetsberättelse

Avseende verksamhetsåret 2018

Förord

Information till vårdgivaren

Socialstyrelsen har utfärdat föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården (HSLLF-FS 2016:40). Föreskrifterna innehåller ett stort antal krav som rör vårdgivares arbete med informationssäkerhet. Det gäller t.ex. krav på att vårdgivare är skyldig att utse en eller flera personer som ska leda och samordna arbetet. Den eller de personer som utses att leda och samordna informationssäkerhetsarbetet bör enligt föreskrifterna få en sådan ställning i organisationen att arbetet kan prioriteras och utföras effektivt.

Det finns även krav på att den eller de som utses minst en gång om året ska sammanställa information om arbetet till vårdgivaren. I denna PM redovisas arbetet med informationssäkerhet under 2018 samt en kort statusrapport inom de mest centrala områdena.

Ledningens genomgång

Informationssäkerhet är ett av tre sakområden som ingår i ”ledningens genomgång” som årligen genomförs med koncernledningen. Vid ledningens genomgång görs en analys av styrdokument m.m. i ledningssystemet för respektive sakområde och en bedömning av hur verkningsfull denna styrning är.

Patientsäkerhetsberättelsen

Förutom detta innehåller regionens patientsäkerhetsberättelse sedan några år avsnitt om informationssäkerhetsarbetet. Detta är en följd av en ändring av patientsäkerhetslagen.

Västerås den 31 januari 2019

Michael Patriksson

Informationssäkerhetssamordnare

Innehåll

1 Digitalisering

Digitalisering har kommit att bli ett nyckelord och en tydlig strategisk inriktning inom alla sektorer av samhället. Sveriges riksdag och regering arbetar strategiskt med frågan. I media uttalar olika företrädare att Sverige ska ligga i framkant och i vissa fall vara bäst i världen när det gäller digitalisering. En särskild myndighet, Myndigheten för digital förvaltning[1], har inrättats. På liknande sätt utarbetas strategier på regional och lokal nivå inom offentlig sektor, samt naturligtvis inom den privata sektorn.

I de nationella planerna finns tydligt uttalat att informationssäkerhet är en nödvändig förutsättning för att digitaliseringen ska nå sina syften. En sökning med begreppet ”informationssäkerhet” på regeringens hemsida visar ett stort antal dokument med uppdrag till flertalet statliga myndigheter på området att stärka sin förmåga på området. Liknande uttalanden om vikten av informationssäkerhet saknas i stor utsträckning i de planer och styrdokument kring digitalisering som tagits fram inom regionen. Detta medför på sikt allvarliga risker för fel och läckage av person- och patientuppgifter.

2 Övergripande styrdokument

Dåvarande landstingsfullmäktige antog i september 2014 en informationssäkerhetspolicy[2]. Enligt policyn ska regionen bedriva ett systematiskt arbete med informationssäkerhet som bygger på riskanalyser och ständiga förbättringar., liksom att inriktningen är att följa den internationella standarden ISO/IEC 27001.

Policyn innehåller även tio centrala principer, som bl.a. handlar om vikten av informationsklassning, säkerhet i it-drift och förvaltning samt värnande av personlig integritet.

Slutligen finns ett avsnitt om roller och ansvar där detta klargörs för fullmäktige, styrelse, regiondirektör, chefer och medarbetare samt att det ska finnas ett Informationssäkerhetsråd som har ansvar för samordning och utveckling.

Informationssäkerhetspolicyn revideras och en uppdaterad version kommer att tillställas regionfullmäktige för fastställelse under 2019.

[1] https://www.digg.se/
[2] http://ledningssystemet/anonym/ViewItem.aspx?regno=8490

3 Riskanalyser

Informationssäkerhetssamordnaren har under åren i genomsnitt genomfört ca tjugo riskanalyser per år. Sedan maj 2018 ingår informationssäkerhet som ett av nio målområden i Västmanlands integrerade metod för riskanalyser, VIRA. Under 2018 utbildades drygt 70 analysledare i metoden, vilket medfört att risker på informationssäkerhetsområdet identifieras och värderas i en helt annan omfattning än tidigare. Detta blev också nödvändigt med tanke på de utökad krav på riskanalyser som följde med ikraftträdandet av Dataskyddsförordningen, se särskilt avsnitt 6 nedan. Genom ett integrerat arbetssätt med riskanalyser öppnas även möjligheten för ledningen att få en sammanhållen bild av verksamheternas riskbild.

Under 2019 går arbetet med VIRA vidare, där fokus kommer att ligga på riskhantering, dvs. rutiner för att hantera och ta fram åtgärder för att minimera de identifierade riskerna alternativt lindra konsekvenserna i de fall risken realiseras.

4 Informationsklassning

Region Västmanland har sedan 2015 en metod där information i it-relaterade tjänster klassas. Klassningen går till så att det görs en bedömning av vilken skada om skulle uppstå om informationen förlorar

- Konfidentialitet (informationen blir tillgänglig för obehöriga)
- Riktighet (informationen innehåller fel)
- Tillgänglighet (informationen är inte tillgänglig för användarna, ”systemet ligger nere”)
- Spårbarhet (loggningen upphör att fungera).

När klassningen gjorts kan ansvariga sedan granska tekniska krav som Centrum för digitalisering tar fram för respektive klass och jämföra det med de faktiska skydd som lösningen innehåller. På detta sätt kan tekniska skydd tillföras it-lösningen på ett strukturerat sätt och inte som tidigare mer vanligt ”ad hoc”. Vinsten ligger i att regionen kommer nära målet att tillföra rätt säkerhet, att inte missa att skydda känslig information samt att inte överinvestera i säkerhet.

Under 2018 var samtliga ca 500 system och tjänster inom regionen klassade och de tekniska skydden i allt väsentligt avstämda mot de tekniska skydd som följer av klassningen.

Det är av mycket stor vikt att informationsklassning blir en obligatorisk del vid kravställning i upphandling. Avsikten är att klassning under 2019 ska föras in i den arbetsprocess som tillämpas inom Inköp Sörmland/Västmanland.

5 Dataskyddsförordningen GDPR

I maj 2018 trädde EU:s allmänna dataskyddsförordning (GDPR) ikraft och ersatte då Personuppgiftslagen som gällt i Sverige sedan 1998. För regionens del innebar den nya lagstiftningens inte så många nyheter, mycket handlade om att förtydliga regler som gällt sedan tidigare. De viktigaste nyheterna gällde främst:

- Krav på obligatoriska riskanalyser vid förändring eller nyanskaffning av it-relaterade tjänster som innehåller känsliga personuppgifter, t.ex. patientuppgifter.
- Skyldighet att samråda med regionens dataskyddsombud inför förändringar eller anskaffning av sådana lösningar.
- Skyldighet att skyndsamt, senast inom 72 timmar, anmäla incidenter till Datainspektionen och underrätta drabbade av sådana incidenter.
- Krav på s.k. inbyggt dataskydd i it-relaterade tjänster, vilket bl.a. medför att de system etc. som regionen använder nte får innehålla överflödig information, att de måste innehålla funktioner för loggning och autentisering av användare m.m.
- Möjlighet för Datainspektionen att utfärda administrativa böter vid brott mot reglerna, upp till 20 miljoner kronor för offentliga organisationer i Sverige. Dessa kan utfärdas vid flera tillfällen, så länge inte rättelse skett.

Intresset för GDPR var mycket stort bland regionens medarbetare. Informationssäkerhetssamordnaren anordnade därför en föreläsningsserie där närmare 500 chefer och medarbetare från olika verksamheter deltog.

Med den nya lagstiftningen vaknade även insikten om de brister som funnits under den tid då personuppgiftslagen gällt. Det handlade bl.a. om avsaknaden av personuppgiftsbiträdesavtal som måste finnas då externa leverantörer behandlar regionens personuppgifter (t.ex. vid utkontraktering eller anlitande av s.k. molntjänster). Mycket arbete ägnades därför åt att ta fram och teckna avtal med leverantörer i de stora antal fall där detta saknats. Vid ingången av 2019 saknas fortfarande biträdesavtal med ett mindre antal leverantörer och avsikten är att dessa ska hanteras under 2019. Ett problem i sammanhanget är dock att det största motståndet mot att teckna avtal med avtalsvillkor som de flesta regioner och även SKL enats kring finns hos några av största programvaruleverantörerna. De vill ogärna teckna villkor som innebär att de tar ansvar för fel, att de kan utsättas för revision eller tvingas uppge när de anlitar underleverantörer.

6 NIS-direktivet

I november 2018 trädde ett EU-direktiv om informationssäkerhet i samhällsviktiga och digitala tjänster ikraft, det s.k. NIS-direktivet. Direktivet har implementerats i

svensk lagstiftning genom lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster. Av regionens verksamhetsområden omfattar lagen hälso- och sjukvården samt kollektivtrafikförvaltningen.

Till skillnad från GDPR, som handlade om att skydda personuppgifter från obehörig åtkomst, handlar NIS-direktivet om att organisationer ska ha sådan grad av informationssäkerhet att störningar inte uppkommer i samhällsviktiga tjänster. För regionens del handlar det t.ex. om att it-system som är centrala för vården ska vara tillgängliga för verksamheterna när de behövs. Det kan vara journalsystem, röntgensystem, viss medicinteknisk utrustning m.m.

NIS-direktivet omfattar även samhällsviktiga transporter, där stora delar av den verksamhet som bedrivs inom Kollektivtrafikförvaltningen ingår.

Direktivet och den svenska lagstiftningen kompletterades sent 2018 med föreskrifter från Myndigheten för samhällsskydd och beredskap (MSB)[3]. Analys och framtagande av nödvändiga riktlinjer och rutiner kommer att utarbetas inom informationssäkerhetsgruppen inom sjukvårdsregionen (den s.k. 7-klövern) under 2019.

7 Informationssäkerhet i drift och förvaltning

En viktig del av informationssäkerhetsområdet är it-säkerhet. En särskild riktlinje om detta utarbetades och fastställdes i juni 2018. Riktlinjen ”It-säkerhet i drift och förvaltning[4]” innehåller en heltäckande reglering i frågor som rör t.ex. nätverkssäkerhet, virusskydd, säkerhetskopiering, oberoende granskning och tekniska krav på serverhallar.

Riktlinjen är implementerad i de driftrutiner m.m. som tillämpas inom Centrum för digitalisering och används även som underlag för granskningar av it-säkerheten, i exempelvis serverhallar.

8 Säkerhetskultur

Den grad av medvetenhet om informationssäkerhet och risker m.m. som personalen i en given organisation har brukar kallas ”säkerhetskultur”. Överlag inom regionen måste säkerhetskulturen klassas som bristfällig. Det finns, särskilt inom vårdverksamheten, ett motstånd mot olika former av tekniska eller administrativa skydd. Dessa upplevs som ”krångliga” eller som ett allvarligt hinder i arbetet. Ett särskilt tydligt exempel är det arbete som drivits under flera år för att införa rutiner

[3] https://www.msb.se/sv/Om-MSB/Nyheter-och-press/Nyheter/Nytt-informationssakerhet/Nya-foreskrifter-kopplade-till-NIS-regleringen-/
[4] http://ledningssystemet/anonym/ViewItem.aspx?regno=27906

för säker identifiering av användare i huvudjournalsystemet. Det handlar där om att uppfylla tydliga krav som funnits i över tio år i lagstiftningen, samt upprätthålla invånarnas förtroende för att regionen efterlever kraven på personlig integritet och säkerhet. Efter mycket arbete och stort engagemang från många chefer och medarbetare verkar frågan få en lösning i maj/juni 2019.

En förbättring av säkerhetskulturen kan uppnås genom olika informationsinsatser, men även genom att erbjuda lösningar som inte upplevs som hinder i verksamheterna. Detta kräver ett långsiktigt och tämligen resurskrävande arbete. I den kartläggning och analys som MSB genomförde 2018[5] kunde regionen svara jakande på sju av åtta frågeställningar som ingick i undersökningen. På den åttonde, som handlade om tillräckliga resurser för informationssäkerhetsarbetet, blev svaret nekande.

9 Logguppföljning

I egenskap av vårdgivare har regionen ett lagstadgat ansvar för att åtkomst till patientuppgifter i it-system följs upp och kontrolleras.

Rutinerna kring loggranskning har genomgått stora förändringar de senaste fyra åren. Tidigare rutiner var dels mycket arbetsdryga, dels hade de extremt dålig träffsäkerhet när det gällde att hitta misstänkta överträdelser mot regelverket kring åtkomst.

Det inleddes därför ett arbete för att så långt möjligt automatisera kontrollerna och förenkla rutinerna så att mindre tid behövde läggas på denna uppgift. I de internkontroller som genomfördes åren 2014-2017 visade det sig att antalet verksamheter som efterlevde riktlinjerna kring loggranskning ökade från drygt 30 procent till nästan 95 procent. Samtidigt ökade träffsäkerheten i de automatiserade kontrollerna mångfalt.

Den övergripande målsättningen för regionens arbete med loggranskning är att upprätthålla invånarnas förtroende för att medarbetarna hanterar patientuppgifter i enlighet med gällande lagar och föreskrifter. Ett annat mål är att alla medarbetare ska känna till reglerna för åtkomst så att ingen ska kunna misstänkas för att olagligen ha öppnat journalen för en patient. Under senare år uppdagas tio till femton fall per år av misstänkt dataintrång, målsättningen är som sagt att detta ska ner till noll.

[5] https://www.msb.se/sv/Produkter--tjanster/Publikationer/Publikationer-fran-MSB/En-bild-av-landstingens-informationssakerhetsarbete-2018--kartlaggning-och-analys-av-landstingens-informationssakerhetsarbete-inom-halso--och-sjukvardsverksamheten/

10 Revision och uppföljning

Regionrevisorerna har genomfört två granskningen med bäring på informationssäkerhet under 2018. Den ena granskningen rörde specifikt regionens informationssäkerhetsarbete, den andra säkerheten i journalsystemet Cosmic. Regionstyrelsen har behandlat och besvarat rapporterna.

Informationssäkerhet ingår även sedan 2017 som ett av sakområdena i internrevisionen. Revisionsrapporterna speglar bl.a. den bild som redovisats ovan vad avser säkerhetskultur.

Insatser för att följa upp beslutade riktlinjer och instruktioner har främst skett vad avser loggranskning, behörighetshantering samt tecknande av biträdesavtal enligt GDPR.

11 Incidenter

Under 2018 har inga allvarliga incidenter inom informationssäkerhetsområdet inträffat. Som allvarlig incident räknas sådana som påverkat säkerheten i en tjänst eller ett system och som möjliggjort för obehöriga att komma åt, förändra eller förstöra samtliga person- eller patientuppgifter som hanteras i tjänsten/systemet.

12 Deltagande i nätverk

Informationssäkerhetssamordnare deltar i MSB:s nationella nätverk ”Vårdens nätverk för informationssäkerhet” samt ett nätverk för informationssäkerhet och juridik inom sjukvårdsregionen Uppsala-Örebro, den s.k. 7-klövern. I det senare nätverket bedrivs i ökande omfattning gemensamt utvecklingsarbete, framtagande av gemensamma mallar m.m.

Den regionala informationssäkerhetsgruppen i 7-klövern har sedan 2017 formaliserats som en grupp under Samverkansnämnden Uppsala-Örebro sjukvårdsregion. Gruppen tar fram särskild verksamhetsplan och verksamhetsberättelse har även att ta emot uppdrag från regiondirektörerna i Samverkansnämnden.

13 Omvärldsbevakning

Informationssäkerhetssamordnaren samlar genom nätverk och kontakter fortlöpande in händelser med bäring på informationssäkerhet, såväl nationellt som internationellt. Dessa skickas tre gånger i veckan till en särskild sändlista dit intresserade kan anmäla sig. Dessutom driver informationssäkerhetssamordnaren

Informationssäkerhetsbloggen[6] där ett urval av nyheter och händelser publiceras någon gång per vecka.

14 Förbättringsåtgärder

Som nämndes inledningsvis är regionens inriktning att utpekade, internationella standarder på området ska följas. Huvuddelen av de drygt 130 krav som ställs i standarden är uppfyllda. Arbetet under 2019 inriktas på de punkter där det finns brister. Detta gäller bl.a. vissa krav vad gäller åtkomsthantering och kontinuitetshantering.

[6] https://ltvse-my.sharepoint.com/personal/michael_patriksson_regionvastmanland_se/Blog/default.aspx