Regionkontoret
Centrum för administration
Juridik och säkerhet

Datum 2020-02-04
Diarienummer 200232

Regionstyrelsen

Läget inom informationssäkerhetsområdet 2019

Inledning

Vårdgivare är enligt 3 kap. 6 § Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården (HSLF-FS 2016:40) skyldig att utse en eller flera personer som ska leda och samordna informationssäkerhetsarbetet. Den eller de som utses ska minst en gång om året sammanställa information om arbetet till vårdgivaren. Redovisningen för 2019 görs genom denna rapport.

Policy och målsättning om certifieringsbarhet

Enligt informationssäkerhetspolicyn, som fastställts av regionfullmäktige, ska regionens arbete med informationssäkerhet utgå från den internationella standarden ISO/IEC 27001. Regionen ska enligt tidigare beslut i Riskkommittén uppfylla de ca 140 kraven i policyn och därmed vara certifieringsbar.

Under 2019 uppfylldes drygt 130 av dessa krav. Arbetet med återstående krav kommer att fortsätta under 2020. Det som saknas handlar främst om kontinuitet i informationshanteringen.

Säkerhetskultur och informationsinsatser

Insatser för att höja säkerhetsmedvetandet i verksamheterna har fortsatt under 2019. Informationssäkerhetssamordnaren har under 2019 medverkat och informerat på 33 arbetsplatsträffar och liknande sammankomster.

I takt med att medvetenheten om informationssäkerhet ökar i regionens verksamheter ökar också antalet frågor via e-post och telefon. Det är en utveckling som pågått under ett antal år. Att kunna ge ökat stöd till verksamheterna är givetvis positivt men det tar också alltmer resurser.

I oktober genomfördes en särskild satsning i form av en ”informationssäkerhetsvecka”. Under veckan genomfördes föreläsningar under en s.k. sopplunch och en särskild föreläsning kopplad till Dataskyddsförordningen.

Kontaktperson Michael Patriksson, 021-17 65 69, michael.patriksson@regionvastmanland.se

Därutöver togs det fram nytt informationsmaterial på Arbetsplatsen[1] och en folder med allmänna råd kring informationssäkerhet. I informationsmaterialet ingick länkar till Informationssäkerhetsbloggen[2] och till den särskilda filmkanalen för informationssäkerhet[3].

Omvärldsbevakningen har fortsatt under 2019. Drygt 100 nyhetsbrev har skickats ut till berörda medarbetare.

Digitalisering

Regionen strävar, precis som samhället i övrigt, efter att utnyttja de möjligheter till effektivisering som digitaliseringen erbjuder. En digitaliseringsstrategi fastställdes tidigare för åren 2018-2020[4]. I ett informationssäkerhetsperspektiv bör regionens digitaliseringsstrategi tydligt betona vikten av att säkerhetsaspekter beaktas, så som gjorts t.ex. i den nationella strategin utgiven av regeringen[5].
Informationssäkerhetssamordnaren kommer att driva på för att detta beaktas i nästa version av regionens strategidokument.

Inköp

Under året har rutinerna i samband med inköp och upphandling kompletterats med stödmaterial som bl.a. betonar att riskanalys och informationsklassning ska genomföras i syfte att få fram lämpliga krav på informationssäkerhet. Målet är att anskaffade IT-relaterade tjänster ska ha ”rätt säkerhet”, inte för mycket och inte för lite.

Ett närmare samarbete med Inköp har under året även medfört att frågor kring kravställning allt oftare ställs till informationssäkerhetssamordnaren innan förfrågansunderlagen slutligen fastställs, vilket självfallet är positivt.

Stark autentisering i Cosmic

Under året har arbetet med att införa stark autentisering vid inloggning mot huvudjournalsystemet, vilket krävs enligt gällande författningar, fortsatt. Införandet innebär att möjligheten att logga in med enbart användarnamn och lösenord tas bort, istället krävs inloggning med eTjänstekort (SITHS). Regionstyrelsen har i yttrande till regionrevisorerna tidigare utlovat att detta skulle ha kommit på plats under 2019. En rad invändningar har därefter rests från vårdpersonal med hänvisning till patientsäkerheten, vilket lett till att ett antal riskanalyser genomförts. Ett projekt har tillskapats med uppgift att ta fram den tekniska lösningen. Riktlinjer och instruktioner har tagits fram och är färdiga att utfärda när projektet levererar sin lösning, vilket enligt plan ska ske under första halvåret 2020.

---

[1] https://ltvse.sharepoint.com/ps-vartlandsting/Pages/Informationssäkerhet.aspx
[2] https://ltvse-my.sharepoint.com/personal/michael_patriksson_regionvastmanland_se/Blog/default.aspx
[3] https://web.microsoftstream.com/channel/90e884a9-a7ac-4b18-b764-08071bece510
[4] https://ltvse.sharepoint.com/teams/ARK/Delade%20dokument/PU/strategi-for-digitalisering-av-region-vastmanland.pdf
[5] https://www.regeringen.se/49adea/contentassets/5429e024be6847fc907b786ab954228f/digitaliseringsstrategin_slutlig_170518-2.pdf

Krav på stark autentisering införs även på en rad nationella tjänster, bl.a. Nationell patientöversikt (NPÖ) samt tjänster som tillhandahålls av E-hälsomyndigheten och Inera AB.

IT-säkerhet

Regionens ledningssystem innehåller sedan ett antal år en riktlinje för IT-säkerhet i drift och förvaltning[6]. Under år 2019 har ett arbete drivits med översyn av denna riktlinje samt analys av bakomliggande rutiner, som i några fall inte dokumenterats. Målet med arbetet är att genom förbättrad dokumentation minska nyckelpersonberoenden och uppnå högre grad av robusthet och resiliens. Detta arbete kommer att fortsätta under 2020.

Övningsverksamhet, IT-incidenter

Informationssäkerhetssamordnaren medverkade i planering och genomförande av en övning kring en fingerad IT-incident. Övningen genomfördes med berörd personal inom dåvarande Centrum för digitalisering. Övningsverksamheten kommer fortsätta och skalas upp under 2020 så att samövning kan ske med regionens övriga stabs- och beredskapsfunktioner.

Nätverkande i Sjukvårdsregionen och nationellt

Samarbetet i Sjukvårdsregionen Uppsala-Örebro har fortsatt. Informationssäkerhetssamordnaren har haft ordförandeskapet under 2019 och har fortsatt driva fram konkreta resultat bl.a. inom områdena incidenthantering och dataskydd.

Informationssäkerhetssamordnaren deltar sedan många år i Myndigheten för samhällsskydd och beredskaps nationella nätverk HOSIS (Hälso- och sjukvårdens informationssäkerhetsnätverk). Aktiviteterna i HOSIS inriktas främst på informationsdelning.

Informationssäkerhetsrådet

Informationssäkerhetsrådet har sammanträtt vid fem tillfällen under 2019. I rådet samlas frågor och synpunkter in från verksamheterna samtidigt som nya styrdokument, informationsmaterial etc. remissas innan de beslutas/lanseras. Bland frågor som behandlats i rådet under år 2019 kan nämnas införandet av självbetjäningsterminaler, riktlinjer kring behörighetshantering i journalsystem samt införandet av ny e-utbildning om informationssäkerhet.

Dataskyddsförordningen, GDPR

Under 2019 fortsatte arbetet med att ta fram och teckna s.k. personuppgiftsavtal med externa leverantörer. Dessa avtal är obligatoriska i de fall regionen utkontrakterar behandlingen av personuppgifter. Det har dels gällt att teckna avtal

[6] https://www.regeringen.se/49adea/contentassets/5429e024be6847fc907b786ab954228f/digitaliseringsstrategin_slutlig_170518-2.pdf

där de saknats med befintliga leverantörer samt komplettera rutinerna på Inköp så att personuppgiftsbiträdesavtal alltid ingår vid nya upphandlingar/inköp.

Regionen gjorde anmälan av en incident till Datainspektionen. Det gällde förhållandet att vissa samtal rörande beställning av sjukresor hamnat på samma oskyddade databasserver som var fallet med det mycket stora antalet samtal till 1177 som tagits upp i regionerna Stockholm, Uppsala och Sörmland. Datainspektionen har inte gått vidare med ett granskningsärende mot Region Västmanland. Däremot väntas beslut i ärendet med övriga tre regioner under första halvåret 2020.

Michael Patriksson

Informationssäkerhetssamordnare och dataskyddsombud