Stockholms läns sjukvårdsområde
Sjukvårdsdirektören

ANMÄLAN
2021-03-22

SLSO 2021-0805

Årsrapport informationssäkerhet för verksamhetsåret 2020

Årsrapport informationssäkerhet för verksamhetsåret 2020 överlämnas till nämnden för Stockholms läns sjukvårdsområde för kännedom.

Region Stockholm

Stockholms läns sjukvårdsområde

ÅRSRAPPORT
2021-03-22

SLSO 2021-0805

Årsrapport informationssäkerhet

För verksamhetsåret 2020

Innehållsförteckning

1. Inledning 3

2. Informationssäkerhetsorganisation 3
2.1 Bedömning 3
2.2 Åtgärd 3

3. Identifiering av skyddsvärd information 3
3.1 Bedömning 4
3.2 Åtgärd 4

4. Utbildning 4
4.1 Bedömning 4
4.2 Åtgärd 5

5. Compliance – regelefterlevnad 5
5.1 Bedömning 5
5.2 Åtgärd 5

6. Styrdokument 5
6.1 Bedömning 6
6.2 Åtgärd 6

7. Incidentrapportering 6
7.1 Bedömning 7
7.2 Åtgärd 7

8. Omvärldsbevakning 8
8.1 Bedömning 8
8.2 Åtgärd 8

9. Konklusion 8

1. Inledning

Regionstyrelsen i Region Stockholm beslutade 2016-02-23, § 55, att anta ett handlingsprogram för informationssäkerhet för åren 2016-2020 (LS 1308-1044). Genom handlingsprogrammet höjdes ambitionsnivån för informationssäkerhetsarbetet inom Region Stockholm.

Stockholms läns sjukvårdsområde (SLSO) har brutit ner målen i handlingsprogrammet i delmål och åtgärder för att uppnå intentionen med handlingsprogrammet. I detta dokument redovisas SLSO:s informationssäkerhetssamordnares iakttagelser och arbete under verksamhetsåret 2020.

2. Informationssäkerhetsorganisation

För att underlätta och förbättra det systematiska arbetet med informationssäkerhet behöver SLSO skapa en organisation där informationssäkerhetskoordinatorer och informationssäkerhetsombud ingår på vårdområdes- och verksamhetsstödsnivå samt vid behov på RE-nivå.

Tillsammans med informationssäkerhetssamordnaren och Dataskyddsombudet ska dessa koordinatorer och ombud samordna arbetet med informationssäkerhet samt arbete kopplat till dataskyddsförordningen inom respektive vårdområde och verksamhetsstöd.

2.1 Bedömning

Arbetet med utformning av en informationssäkerhetsorganisation i syfte att bygga upp lokala stöd- och resurspersoner påbörjades av SLSO:s informationssäkerhetssamordnare under 2020 men fick av förklarliga skäl stå tillbaka under pågående pandemi.

2.2 Åtgärd

Givet en förhoppning att den ansträngda arbetssituationen under pågående covid-19 pandemi förbättras så behöver informationssäkerhetssamordnare driva på arbetet i skapandet av en informationssäkerhetsorganisation.

3. Identifiering av skyddsvärd information

Skyddsvärd information inom SLSO behöver identifieras och klassificeras i syfte att värdera informationen så att tillräcklig nivå av säkerhetsåtgärder finns kopplat till respektive informationsskälla. Detta arbete ger SLSO en

ökad trygghet gällande informationstillgångarnas tillgänglighet, riktighet och konfidentialitet.

3.1 Bedömning

Under 2020 togs en förteckning över SLSO:s IT-system fram i samarbete med VS eHälsa & IT och VIR-projektet. Förteckningen behöver bearbetas ytterligare i syfte att identifiera och prioritera system utifrån skyddsvärdet på informationen som behandlas.

På längre sikt finns behov av arbete med att etablera en process för inventering och förteckning av informationstillgångar och som en del av processen identifiera systemägare för SLSO:s mest kritiska system samt klassificera och granska systemen enligt compliance-processen.

3.2 Åtgärd

Informationssäkerhetssamordnarna ser ytterligare behov av att arbeta med SLSO:s systemförteckning, en första åtgärd är att skriva ett projektförslag för genomförande av identifiering och förteckning av skyddsvärda system under 2021.

En annan planerad åtgärd under 2021 är att arbeta tillsammans med enheten för informationssäkerhet vid Regionledningskontoret med att ta fram en modell för att identifiera den mest skyddsvärda informationen.

4. Utbildning

SLSO:s medarbetare ska visa upp en medvetenhet och ett kunnande gällande informationssäkerhet vilket medför att utbildning och kommunikation måste vara en integrerad del i all utveckling och implementation av ett systematiskt informationssäkerhetsarbete.

Datorstödd informationssäkerhetsutbildning för användare (DISA) är Region Stockholms grundutbildning i informationssäkerhet vilken även är obligatorisk för alla medarbetare inom Region Stockholm. DISA-utbildningen är ett led i att öka medvetenheten och kunskapen om informationssäkerhet och SLSO ska arbeta för att alla medarbetare genomför utbildningen.

4.1 Bedömning

Genomförandegraden för SLSO:s medarbetare för den obligatoriska DISA-utbildningen är förhållandevis låg (30 % för åren 2017-2020, under 2020 10 %).

För att förstärka medvetenheten genomfördes under hösten 2020 en utbildningssatsning genom nanolearning i informationssäkerhet för de medarbetare som inte arbetar patientnära. Nanolearning som metodik syftar till ökat medvetande genom kontinuerligt lärande. För kursen bestående av 13 utskickade lektioner låg genomförandegraden betydligt högre, 60 % hade genomfört 85-100% av lektionerna.

4.2 Åtgärd

Under 2021 kommer åtgärden primärt vara olika kommunikationsinsatser i syfte att öka genomförandegraden av den obligatoriska grundutbildningen i informationssäkerhet, DISA.

5. Compliance – regelefterlevnad

Compliance-portalen är Region Stockholms IT-stöd för systematiskt informationssäkerhetsarbete. Med hjälp av Compliance-portalen går det att göra egenkontroller och följa upp SLSO:s informationssäkerhetsarbete. Compliance-portalen ger en bild av hur både verksamheter och IT-system efterlever Region Stockholms riktlinjer för informationssäkerhet (regelefterlevnad). Resultatet i Compliance-portalen kan användas för att identifiera förbättringsområden och ta fram förslag på åtgärder så att SLSO:s information skyddas på rätt sätt. Genom att arbeta i verktyget skapas förutsättningar för ett systematiskt och långsiktigt arbete inom området.

5.1 Bedömning

Arbetet med regelefterlevnadsgranskningar av såväl IT-system som verksamheter inom ramen för den s.k. Compliance-processen har fortskridit enligt den framtagna handlingsplanen för verksamhetsåret 2020, där de uppsatta målen är uppnådda och mer därtill.

5.2 Åtgärd

Arbetet med regelefterlevnadsgranskningar fortsätter enligt handlingsplan för kommande år.

6. Styrdokument

Styrdokument är viktig del av arbetet med informationssäkerhet då informationssäkerhetssamordnarnas arbete utgår från dessa samt att SLSO måste kunna visa att organisationen lever upp till riktlinje och policy för informationssäkerhet. Under 2020 har beslutet att frångå egen riktlinje och policy tagits för att minska antalet styrdokument. SLSO:s informationssäkerhetssamordnare har deltagit i arbetet med att granska

den nya riktlinjen för informationssäkerhet och policyn för verksamhetsskydd som tagits fram av enheten för informationssäkerhet vid Regionledningskontoret som väntas fastställas under 2021. När dessa är fastställda kommer SLSO att följa de regionalt framtagna riktlinjerna.

SLSO:s arbete med informationssäkerhet utgår främst från följande styrdokument:

- Riktlinje informationssäkerhet
- Policy verksamhetsskydd
- E-postanvändning – övergripande anvisning för SLSO

För att SLSO ska kunna bedriva ett systematiskt och kvalitativt informationssäkerhetsarbete krävs att relevant information finns lättillgänglig för alla medarbetare, därav finns samtliga styrdokument samlade för anställda att ta del av på intranätet samt i ärende- och dokumenthanteringssystemen Dokumenta/Platina.

6.1 Bedömning

SLSO:s informationssäkerhetssamordnare bedömer att beslutet att frångå egen riktlinje och policy och istället följa de regionalt framtagna styrdokumenten kommer att underlätta arbetet med samordning såväl som arbetet ute i verksamheterna då antalet styrdokument minskar och har en gemensam inriktning över hela Region Stockholm.

Vidare tillkommer tillämpningsanvisningar under 2021 för att kunna applicera innehållet i riktlinjen i verksamheterna vilket ytterligare kommer att underlätta arbetet.

6.2 Åtgärd

Ytterligare översyn av styrande dokument när de är fastställda i syfte att identifiera om behov finns av förtydliganden eller lokala anpassningar för implementering inom SLSO.

Parallellt med översynen av nyframtagna dokument kommer också en översyn av befintliga lokala styrdokument genomföras.

Kommunikationsinsatser för att förmedla information om nya riktlinjer kommer att ske framförallt via intranätet Insidan.

7. Incidentrapportering

Incidenthantering via Helpdesk omfattar alla händelser som stör eller kan störa IT-miljön oavsett om händelsen sker hos SLSO eller underleverantör. Detta inkluderar händelser som rapporteras in såväl av användarna som av tekniker som upptäcker avvikelser från normal IT-drift.

Inkommande incidenter anses vara en informationssäkerhetsincident vid en klassificering av 1 (kritisk) eller 2 (hög) enligt fastställd prioriteringsmatris som HelpDesk använder sig av. Prioriteringar sker enligt en femgradig skala vilken baseras på incidentens angelägenhet och påverkan för vårdgivare och patientsäkerhet. Prioritering görs i första linjens support och kan vid behov ändras av en incident manager (IM).

Personuppgiftsincidenter rapporteras av verksamheten direkt till Integritetsskyddsmyndigheten (IMY) och dataskyddsombud informeras i samband med rapportering. Förutom den årliga återrapporteringen så rapporteras uppkomna personuppgiftsincidenter i anslutning till ledningsgruppsmöten.

En incidenthanteringsprocess har även under 2020 fastställts för att hantera incidenter enligt NIS-direktivet.

7.1 Bedömning

Incidenthantering har varit en utmaning att arbeta med på grund av avsaknad av systemstöd och process när det gäller informationssäkerhetsincidenter.

Frågan har tagits upp med enheten för informationssäkerhet vid Regionledningskontoret ett flertal gånger under de senaste åren som har bekräftat att det är en regional utmaning och behov. Frågan har även behandlats under informationssäkerhetsrådets möten.

Tiohundra förevisade sin process för hantering av informationssäkerhetsincidenter på ett ISR-möte, ett arbete som har tagit tre år att få till stånd och fortfarande är i etableringsfas inom organisationen.

SLSO:s informationssäkerhetssamordnare följer utvecklingen på regional nivå och SLSO:s bedömning är att det behövs en regional samordning snarare än lokala initiativ kring denna fråga.

7.2 Åtgärd

Påtalar kontinuerligt behovet för enheten för informationssäkerhet vid Regionledningskontoret samt håller SLSO uppdaterade kring utvecklingen på regional nivå.

8. Omvärldsbevakning

Omvärldsbevakning är av stor vikt för att hålla sig a jour med arbete inom området informationssäkerhet och även vad gäller dataskyddsförordningen.

En noterbar händelse under 2020 var IMY:s granskning av åtta vårdgivare, däribland SLSO:s vårdgrannar Karolinska Universitetssjukhuset och Capio S:t Görans Sjukhus, gällande personalens åtkomst till journaluppgifter.

8.1 Bedömning

I omvärldsbevakningssyfte har informationssäkerhetssamordnare deltagit i nätverksträffar och utbildningar samt bevakat praxis och nyheter och informerat berörda när informationen varit relevant för dem.

Gällande IMY:s granskning i vårdsektorn ansågs bristerna vara så pass allvarliga att de utmynnade i sanktionsavgifter om 4 respektive 30 miljoner kronor för Karolinska Universitetssjukhuset och Capio S:t Görans Sjukhus. SLSO följer utvecklingen och aktiviteter som följer av granskningen och eventuella överklaganden.

8.2 Åtgärd

SLSO följer utvecklingen till följd av IMY:s beslut och ett arbete med en behovs- och riskanalys inom hälso- och sjukvården för SLSO kommer att initieras under 2021.

9. Konklusion

För att öka medvetenheten och kunskapen om informationssäkerhet genomfördes e-learning kurser i informationssäkerhet med målgrupper chefer samt administrativa medarbetare inom SLSO under 2020. Det krävs fortsatt fokus på att öka medvetenhetande och kunnandet inom organisationen genom utbildningsinsatser samt upprättande av nya rutiner.

Arbetet med utformningen av en informationssäkerhetsorganisation i syfte att bygga upp lokala stöd- och resurspersoner har försenats på grund av covid-19, det kan konstateras att förseningen har haft negativ inverkan på framfarten för arbetet inom området. Detta kommer följas upp under 2021.

Arbetet med informationssäkerhet har i övrigt fortskridit enligt den framtagna handlingsplanen där måluppfyllnaden har överträffats för 2020. Som en del av handlingsplanen genomförs kontinuerligt regelefterlevnadsgranskningar av såväl IT-system som verksamheter inom ramen för den s.k. Compliance-processen. Handlingsplanen för informationssäkerhet revideras och uppdateras årligen och kommer

fortsättningsvis ha ett långsiktigare perspektiv över en treårsperiod med syfte att hantera risken att inte leva upp till Region Stockholms riktlinjer.

En uppdaterad inventering av SLSO:s IT-system i syfte att kartlägga dessa genomfördes under våren 2020, det finns behov av att arbeta vidare med identifiering och förteckning av skyddsvärda system under 2021.

Rapporteringssätt och regelbundenhet av detsamma kan utökas och utvecklas om SLSO:s nämnd så önskar.

Stockholm, mars 2021

Sara Daniels-May
Informationssäkerhetssamordnare

Henrik Strand
Informationssäkerhetssamordnare