Regionkontoret
Centrum för administration
Juridik och säkerhet
Moon Carlbring

Datum 2022-04-06
Diarienummer XXXXXX
Dokumenttyp: Rapport

Verksamhetsrapport informationssäkerhet 2021

Inledning

Krav på att det finns ett strukturerat informationssäkerhetsarbete återges i flertal författningar så som Socialstyrelsen föreskrift om hälso- och sjukvården (2016:40) och Patientdatalagen (2008:355)

En gång per år ska informationssäkerhetsarbetet redovisas för vårdgivaren. Denna rapport redovisar informationssäkerhetsarbetet under 2021.

Styrdokument och certifieringsbarhet

Det finns idag en informationssäkerhetspolicy som är fastställd av regionfullmäktige sedan 2019. Inriktningen för regionens informationssäkerhetsarbete är att den ska vara systematisk och att det ska beröras av alla verksamheter.

Informationssäkerhetsarbetet utgår ifrån standarden ISO/IEC27001 där man under 2019 bedömde att man uppfyllde 130 av 140 krav som återges i standarden. Hur kraven uppfyllts har saknat en tydlig spårbarhet och har varit svårt att följa upp.

Idag finns det 33 styrdokument i ledningssystemet som ska återspegla styr- och stöddokument för informationssäkerhetsarbetet. I de 33 styrdokumenten är det en otydlig återspegling över ISO/IEC27001 vilket kommer prioriteras framöver.

Revisioner och tillsyn

Under 2021 har regionen genomgått två externa revisioner samt en tillsyn.

En extern revision utfärdades av Internetstiftelsen på uppdrag från E-hälsomyndigheten för regionens IdP (identity provider. identitetshantering) som ges tillgång till de nationella vårdtjänsterna som är kopplade till myndigheten. Ett

antal styrdokument reviderades, riskanalysen som begärdes in i samband med revisionen kompletterades vid ett senare tillfälle.

Region Västmanland är anslutna till flera av Ineras vårdtjänster och använder i samband med det identifieringstjänst SITHS för att identifiera sig. Inera AB utförde en extern revision mot regionens SITHS-arbete. Övergripande resultat från revisionen är att regionen har en hög kompetens och förståelse för informationssäkerhetsarbetet samt hög mognad och genomtänkt ID-administrering. I samband med revisionen framkom 6 mindre avvikelser kopplat till fysisk korthantering och det systematiska riskhantering.

Tillsyn om efterlevnaden av lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster genomfördes av Inspektionen för vård och omsorg. Tillsynen är pågående och ej avslutad.

Riskanalyser

Arbetet med riskanalyser har fått ett genomslag i regionen och riskanalyser genomförs systematiskt i samband med nyanskaffning eller större förändring. Dock saknas systematiken när det inte är samband med nyanskaffning eller större förändringar vilket har återgetts i de två externa revisioner som genomfördes under 2021.

Under 2021 identifierades att riskanalys för SITHS-hantering och NIS-direktiv är två riskanalyser som utifrån lag och överenskommelser måste bedrivas systematiskt och/eller årligen.

Informationsinsatser

Under 2021 har inte informationsinsatser kunnat utföras i samma utsträckning som tidigare. Det har dock funnits ett större behov och efterfrågan av utbildning/information inom sakområdet GDPR och informationsinsats har prioriterats därefter.

Under oktober månaden genomfördes en informationsinsats i linje med den nationella informationssäkerhetskampanjen. Regionen tog fram ett quiz och informationsblad som skickades ut digitalt till samtliga vårdkliniker med möjlighet att skriva ut och sätta upp inom verksamhetens lokaler. Delar av verksamheten har uppskattat materialet och återgett positiv återkoppling.

Under 2021 har också information och stödmaterial utvecklats så att det finns tillgängligt på intranätet och i ledningssystemet.

Inköp

Under 2021 har informationssäkerhetsfunktion i regionerna Västmanland och Södermanland haft ett intensivt samarbete med den gemensamma inköpsfunktionen. Flertal inköp och upphandlingar berör informationssäkerhets- och dataskyddskrav. Förhandling om informationssäkerhets- och dataskyddskrav efter påtecknat affärsavtal har inneburit onödiga förhandlingar och kostnader för verksamheten. Tillsammans med Region Sörmland och inköpsenheten har vi tagit fram en arbetsprocess och stödmaterial för att säkerställa att säkerhetskrav beaktas i hela anskaffningsprocessen.

Dataskydd och Cybersäkerhet

Inom arbetet för informationssäkerhets har dataskydds- och cybersäkerhetsfrågor tagit större plats. Dels kommer kraven från EU men det är också kopplat till de arbetssätt vi har, och dels omvärlden. Olika hotbilder, hotaktörer och sårbarheter ökar risker och konsekvenser. Säkerhetsfrågor och åtgärder ägs i regel av linjeverksamheten men på grund av de snabba utvecklingar inom området finns det en utmaning i att förvänta sig att verksamheter ska ha kompetens inom området. Vice versa är det svårt för informationssäkerhetsfunktionen att ha ett arbetssätt eller resurser som kan gott stöd till alla verksamheter inom regionen.

Registerförteckning och Konsekvensbedömning med informationsklassning och riskanalyser

Utifrån Dataskyddsförordningen ställs det krav på hur regionen ska och får behandlar personuppgifter. Samtliga personuppgiftsbehandlingar ska förtecknas i ett register. Där det finns höga integritetsrisker för den enskilda ska även en konsekvensbedömning göras och den personuppgiftsansvarige (regionen) har då också en skyldighet att vidta de åtgärder som krävs för att minimera riskerna.

En kartläggning över vilka personuppgifter regionen behandlar kommer behöva göras framöver, i samband med det arbetet kommer stora delar av verksamheten behöva bidra med information. Informationssäkerhetsfunktionen har under 2021 tagit fram stödmaterial för förteckning av personuppgiftsbehandling, högriskbedömning och konsekvensbedömning.

Incidenter

Under 2021 har 9 personuppgiftsinicidenter rapporteras in till regionens dataskyddsombud varav 6 vidarerapporterats till tillsynsmyndigheten IMY, samtliga är avslutande ärenden hos IMY.

Under 2021 har även en så kallad NIS-incident rapporterats till MSB och även den är avslutad.

Regionen har idag ett etablerat arbete med IT-incidenter och även en rapporteringskedja för hanteringen. Dock är risken hög p.g.a. kunskapsbrist att medarbetare i regionen inte kan bedöma när en incident är rapporteringsskyldigt enligt NIS-direktivet eller GDPR-förordningen.

Informationssäkerhetsfunktionen har bistått och diarieført samtliga incidenter.

Loggуppföljning

Loggkoll är ett IT-stöd som regionen har utvecklat för att ge stöd till verksamhetens arbete (enligt PDL kap 4 § 3) med att utföra systematiska och återkommande kontroller om obehörig åtkomst.

Under 2021 har flera förbättringsområden identifierats och har aktivt bearbetats.

Nätverkande

Under 2021 har informationssäkerhetsfunktionen deltagit i det nationella nätverket HOSIS för sjukvården och innehar ordförandeskap.

Aktivt deltagande har också bedrivits i nätverket Sjukvårdsregionen Mellansveriges gemensamma informationssäkerhetsarbete.

Övriga tvärsektoriella samarbetet är bl.a. framtagning av den nya Klassa-verktyget som SKR tillhandahåller och Informationssäkerhetsarbetet som bedrivs av SKR/Inera.

En ytterligare samverkan har bedrivits tillsammans med region Sörmland och Inköpsenheten. Tillsammans har vi tagit fram en anskaffningsprocess som säkerställer rätt hantering av personuppgiftsbehandlingar.

Omvärldsbevakning

Informationssäkerhetsfunktionen har under 2021 haft ett utbrett nätverk där omvärldsbevakning skett via olika medier, nyhetsbrev, RSS-flöden m.m..

Utifrån omvärldsbevakningen kan vi se att kraven från EU-regelverk ökar. Flertal regelverk härstammar från reglering av digitaliseringen som även tar höjd för nya typer av hot, risker och sårbarheter.

Omvärldsbevakning för området informationssäkerhetsarbetet innebär bevakning inom it-teknik, lagstiftning internationellt och utvecklingsarbetet inom informationssäkerhet, vilket i sig är en utmaning. En annan utmaning är att kunna omsätta omvärldsbevakningen till en eventuell implementering i verksamheten.

Den nationella (regeringens) digitaliseringsstrategin och informations- och cybersäkerhetsstrategin pekar tydligt på varandra. I takt med digitaliseringsutvecklingar är säkerhet en förutsättning. Välfärdstekniken är en prioriterad fråga för regering. För att kunna möta den ökande efterfrågan inom äldreomsorg är välfärdsteknik en faktor för att lösa utmaningen. Det förekommer dock en hel del säkerhet-, integritet- och etiska aspekter i den tekniken där många offentliga aktörer saknar beställarkompetens och kontroll över information som tekniken behandlar.