# Informationssäkerhetsberättelse 2017

REGION JÄMTLAND HÄRJEDALEN

Anna-Lena Alfreds
Krisberedskap, säkerhet och m

# INNEHÅLLSFÖRTECKNING

# 1 Informationssäkerhetsarbete 2017

Informationssäkerhetsarbetet har varit ett utmanande och omfattande arbete de senaste åren, detta år har inte varit något undantag. Under våren 2017 rekryterades en informationssäkerhetssamordnare vilket har stärkt och underlättat arbetet. Dominerande inslag under året har varit förberedelsearbete inför den nya Dataskyddsförordning som träder i kraft maj 2018 samt förberedelser inför uppstarten av Office 365. Det senare var inget arbete som var planerat inför 2017 och har bidragit till att andra planerade aktiviteter fått skjutas på framtiden.

Regionen står inför stora utmaningar när det gäller att leva upp till kraven i den nya Dataskyddsförordningen. I september startades därför ett införandeprojekt avseende anpassning till den nya kraven. Arbetet har löpt på men är något försenat. En anledning till det är att inventering av Regionens personuppgiftsbehandlingar har tagit längre tid än planerat och det arbetet behöver fortsätta 2018.

Nya lagar som påverkar informationssäkerhets arbetet är framförallt den nämnda Dataskyddsförordningen. Den ersätter den tidigare Personuppgiftslagen men innehåller också utökade krav gällande t ex registrerades rättigheter, sanktionsavgifter , incidentrapportering. En annan förändring är att den tidigare föreskriften SOSFS 2008:14 om informationshantering i vården har upphört. Sedan mars 2017 har den istället ersatts av HSLF-FS 2016:40, Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården. Nytt är att det numera finns krav på att informationssäkerhet ska vara en del av patientsäkerhetsberättelsen. Sveriges kommuner och landsting har utarbetat en mall med fyra obligatoriska punkter för informationssäkerhet. Emellertid är uppdraget att arbeta med informationssäkerhet mycket mer omfattande än vad som där anges och är inte heller endast riktat mot vårdsystem. Regionen har därför valt att, utöver patientsäkerhetsberättelsen, ha en separat informationssäkerhetsberättelse .

I den nya föreskriften är kravet att vårdgivaren ska utse en eller flera personer som ska ansvara för informationssäkerhetsarbetet oförändrat. Den eller de som har fått denna uppgift ska minst en gång om året till vårdgivaren rapportera vilka:

1. granskningar och skyddsåtgärder av större betydelse som har gjorts i enlighet med informationssäkerhetspolicyn,
2. riskanalyser som har utförts avseende informationssäkerheten, och
3. förbättringsåtgärder som har vidtagits.

Samtidigt som Regionens informationssäkerhetsarbete har tagit stora steg framåt de senaste åren så går utvecklingen inom IT området så oerhört snabbt och de tekniska möjligheterna ökar för all verksamhet inom Regionen. Verksamheterna idag har ett högt IT-beroende och därmed ökar också våra risker och sårbarheter. Prioriterade uppgifter inför 2017 var bl.a. att tydliggöra ansvarsfördelningen för informations- och IT säkerhetsfrågor inom Cosmic

förvaltning samt e-hälsotjänster. En workshop har genomförts och en del förbättrings- och förändringsförslag framkom. Andra genomförda prioriteringar var t ex att utveckla logg verktyget Logpoint och införa det i vårdverksamhet för hantering av loggkontroller i COSMIC samt att genomföra riskanalys för användande av molntjänster. Ett omfattande arbete avseende kontinuitetshantering genomfördes under våren inför en större uppgradering av COSMIC som skedde i maj.

Framtagande av en e-utbildning i informationssäkerhet har också genomförts och en första grundutbildning för samtliga medarbetare i SABA Cloud beräknas vara klart i början av 2018. En riktad utbildning för chefer beräknas vara klar under våren 2018.

Det har under 2017 blivit alltmer tydligt att informationshantering och tillhörande säkerhetsarbete är viktigt och nära kopplat till Regionens arbete med säkerhetsskydd och totalförsvarsplanering. Det stärker Regionens val att organisera informationssäkerhet inom Krisberedskap och säkerhet.

## 1.1 Ledningssystem för informationssäkerhet (LIS)

Ledningssystem för informationssäkerhet (LIS) är en integrerad del av Region Jämtland Härjedalens ledningssystem. Informationssäkerhetsarbetet följer standarden ISO 27001. Fortfarande finns områden där det saknas fullvärdiga regelverk och rutiner t ex för användning av nya mobila arbetssätt för vård och behandling (t ex via telefon appar, mail, video m.m.) Regelverk kring användning av molntjänster har under 2017 utvecklats. Kontinuerligt arbete krävs för att utveckla och hålla ledningssystemet aktuellt.

## 1.2 Ledningens genomgång

I de nya rutiner som fastställts för ledningens genomgång d.v.s. uppföljning av ledningssystemets funktionalitet och ständiga förbättringar ingår nu sedan 2016 också informationssäkerhet vilket är viktigt för att systematiskt kunna arbeta med förbättringar. Vid Ledningens genomgång i slutet av 2016, förordades att Regionen skulle införa KLASSA som systemklassningsmodell och Beredskapschefen gavs i uppdrag att bereda ett beslutsunderlag. Detta genomfördes dock aldrig p.g.a. kritik som senare framförts mot KLASSA som verktyg och ett omtag har därav fått göras med verktyg för informations- och systemklassning (se 3.2 Informationsklassning)

Ledningens genomgång genomfördes under våren och fokus för informationssäkerhet var bl.a. information kring de nya föreskrifterna från Socialstyrelsen samt Dataskyddsförordningen. Ett viktigt område som också lyftes fram är distansarbete och molntjänster som ökar i omfång, där poängterades vikten av att riskbedömningar och informationsklassningar behöver stärkas för att t ex säkerställa lagenlig personuppgiftsbehandling innan nya tjänster tas i bruk.

Under hösten prioriterades dessvärre ledningens genomgång bort beroende på bristen på internrevisorer.

## 1.3 Handlingsplan för informationssäkerhet

Då informationssäkerhet är ett komplext och svårt område som till viss del fortfarande saknar effektiva processer har behovet av en övergripande handlingsplan bedömts som fortsatt nödvändigt. En ny tvåårig handlingsplan har därav utarbetats för åren 2018 - 2019. Fokus i den är fortsatt aktiviteter inom lagefterlevnad av personuppgiftshantering men också kontinuitetshantering och säkerhet inom systemförvaltning. Gällande personuppgiftshantering behöver förvaltningarna fortsätta arbetet med inventering av sina behandlingar av personuppgifter inklusive nödvändiga skyddsåtgärder. Samtliga förvaltningar ska också ha utsett informationssäkerhetsombud för sina huvudverksamheter. För Hälso- och sjukvårdsförvaltningen samt regionstaben ska informationsklassning och riskanalys för sex utvalda kritiska IT-system göras. Kopplat till det görs också översyn huruvida ändamålsenliga reservrutiner finns. För Hälso- och sjukvårdsförvaltningen poängteras också att loggkontroller ska utföras i vårdsystemen.

# 2 Riskanalyser och egenkontroll

## 2.1 Revision avseende informationssäkerhetsarbetet

Revisorerna för Region Jämtland Härjedalen genomförde i slutet av 2016 en förstudie med syfte att kartlägga och bedöma om det fanns anledning att besluta om en fördjupad granskning om hur informationssäkerhetsarbetet organiserats och bedrivs i Regionen. Förstudien visade att det pågår ett aktivt arbete mot målet att säkerställa informationssäkerheten, men det konstaterades samtidigt att finns en mängd kända brister av varierande allvarlighetsgrad. Revisorerna ansåg vidare att åtgärder vidtas löpande men inte i tillräcklig takt. Regionstyrelsen rekommenderades att särskilt bevaka några mycket angelägna förbättringsområden.

Ett sådant område är utvecklingen av ett systematiskt arbete gällande informationssäkerhet som ger förutsättningar för att tillräcklig säkerhet uppnås. Där är den övergripande handlingsplanen ett sätt att etablera systematik och struktur. Ett annat sätt är ledningens genomgång, där ledningssystemets funktionalitet lyfts upp i förvaltningsledningarna samt Regionledningen. En ambition för den nya informationssäkerhetssamordnaren är också att etablera ett mer riskbaserat arbetssätt inom informationssäkerhet. Den övergripande riskanalys som tidigare saknades har också genomförts (se 2.2). Rekryteringen av en informationssäkerhetssamordnare borgar också för att öka möjligheten både till att ge stöd ut till verksamheterna men också att följa upp informationssäkerhetsarbetet.

Ett annat område handlar om att inventering av säkerhetsproblem sker på ett ändamålsenligt sätt. För att öka säkerhetsmedvetandet är medarbetarutbildning viktigt och en sådan e-utbildning beräknas vara klar i början av 2018. Inom detta område är också informationsklassning och systemförvaltningsarbete av stor vikt. Arbetet med informationsklassning pågår.

När det gäller systemförvaltning så har Regionen sedan många år en decentraliserad modell för systemförvaltning. Det innebär att det finns många systemägare ute i verksamheterna och förvaltningsarbetet bedöms sammantaget vara eftersatt. Brister finns även i

uppföljningen av säkerhetsåtgärder samt i form av avsaknad av riskförebyggande arbete. Arbetet sker i stor omfattning per system och flera systemägare saknar stöd för säkerhetsarbetet, det finns inte heller något gemensamt forum för systemförvaltare. Modellen bidrar också till svårigheter att peka ut informationsägare. Någon förändring av systemförvaltningsmodellen är inte genomförd, IT chefen bedömer att det skulle öka kostnaderna och det har därmed avvaktats med tanke på den svåra ekonomiska situation som råder. För enstaka system t ex COSMIC har dock en PM3 liknande modell införts och det planeras även för Office 365.

Slutligen pekade förstudien på vikten av att säkerställa att prioriterade åtgärder vidtas. De enskilt viktigaste åtgärderna som har vidtagits för att säkerställa detta är rekryteringen av informationssäkerhetssamordnaren samt att budget avsatts 2018 för informationssäkerhetsarbetet och förberedelser för Dataskyddsförordningen.

## 2.2 Övergripande riskanalys avseende informationssäkerhet

Under året har en övergripande riskanalys för området informationssäkerhet inom Region Jämtland Härjedalen genomförts. Analysen har delats upp i två delar:

1. De största riskerna i det systematiska arbetssättet för informationssäkerhet
2. De mest framträdande specifika operativa riskerna för regionens informationshantering

Del ett visar på betydande risker i hur säkerhetsarbetet bedrivs och att det fortfarande finns en avsaknad av systematik. Detta resulterar i ett ad-hoc-baserat arbetssätt där berörda inte har en medvetenhet i hur de ska planera och genomföra säkerhetsarbetet. Primärt är att regionledningen ska ha kännedom om vilka de största riskerna är och hur de ska åtgärdas och prioriteras. Idag saknas en sådan överblick vilket gör att det är svårt att fatta välgrundade beslut om vilka säkerhetsåtgärder som ska prioriteras. Informationssäkerhetssamordnaren har här en viktig uppgift att bidra till struktur, systematik samt föreslå åtgärder och inriktning. Arbetet kan också förbättras med hjälp av utbildning och mer processinriktat arbete.

En annan hög risk som identifierats är att det är oklart vilka i organisationen som innehar rollen som informationsägare och därmed ska krav ställa på och följa upp säkerheten. Denna roll behöver tydliggöras mer för att kunna fånga upp frågor om säkerheten i högre grad än idag. Det här ställs på sin spets när det gäller den pågående anpassningen till EU:s nya dataskyddsförordning vilken skapar större behov av tydlighet gällande vem som äger informationen och därmed ska ställa krav på informationshantering. Även för att förebygga denna risk är ett processorienterat arbetssätt viktigt.

Del två innehåller de viktigaste operativa riskerna i informationshanteringen för regionen. Riskerna med högst bedömt riskvärde är:

1. Avsaknad av utbildningsinsatser för medarbetare inom informationssäkerhet
2. Brister i arbetssätt, organisation och roller för systemförvaltning av regionens IT-system

3. Brister i styrning och uppföljning av höga (privilegierade) behörigheter
4. Bristande arbetssätt för riskbaserad styrning av säkerheten i informations-hanteringen inklusive systemförvaltning
5. Risker för angrepp av skadlig kod via nätfiske med ”ransomware” vilket skapar risker att information blir otillgänglig och raderas eller läcker till obehöriga

Identifierade konsekvenser som kan bli verklighet av dessa ”6-i-topp”-risker är omfattande och kan innebära väsentliga kostnader för regionens verksamheter. Det finns all anledning att följa dessa risker över tid. En åtgärdslista som ska stödja förbättringsarbetet har tagits fram. Ett flertal riskreducerande åtgärder är påbörjade t ex inom risk för angrepp av skadlig kod samt uppföljning av höga behörigheter.

## 2.3 Informationsklassning och laglighetskontroll för Office 365

Samtliga verksamheter inom regionen och regionens förtroendevalda ska under 2018 börja använda samarbetsplattformar i Microsoft Office 365-tjänsten, anskaffad av regionen under 2017. Tjänsten innehåller bland annat e-post, kalenderfunktion, distansmöten och teamsamarbete.

Under införandeprojektet för tjänsten har en laglighetskontroll utförts baserat på avtalsvillkor och planerat arbetssätt för tjänsten. Delar av tjänsten levereras i form av en molntjänst där regionens information kommer att lagras på extern lagringsyta utanför regionens egna lokala IT-miljö. Delar i laglighetsprövningen har varit informationsklassning, risk- och sårbarhetsanalys samt granskning av avtalsvillkor för att verifiera lagefterlevnad för bland annat laglig hantering av personuppgifter.

Riskanalysen har identifierat att följande övergripande riskområden behöver hanteras:

- Handhavanderisker – att användaren använder tjänstens delar på fel sätt (i strid med gällande rutiner)
- Avtalsrisker – att avtalsvillkor inte uppfyller gällande lagkrav och verksamhetskrav eller att leverantören använder regionens information för egna ändamål
- Tekniska risker – exempelvis att tjänsten och den information den lagrar blir otillgänglig

Användandet av Office 365-tjänsten innebär att nya arbetssätt ska börja användas. Utbildning och goda rutiner blir extra viktigt genom att EU:s dataskyddsförordning träder i kraft under våren 2018. För att minska handhavanderiskerna krävs att regionens medarbetare får utbildning i hur tjänsten/apparna ska användas och att användarstöd finns tillgänglig när den behövs. Användarna behöver utbildning och kunskap om bland annat personuppgiftsbehandling och vart man lagrar, respektive inte lagrar, känslig information.

Ett område som kräver extra fokus gällande utbildning och regelverk är användningen av Office-tjänsten/appar på mobila enheter (smartphones och läsplattor). Mobila enheter har tidigare endast använts för att nå e-post. I den nya tjänsten kommer betydligt mer att finnas tillgängligt via mobila enheter d.v.s. både e-post, dokument, kommunikation i form av skype. Regionen behöver också ställa vissa krav vid användning av privata mobiler.

En avtalsgranskning av Regionens avtal med Microsoft har också utförts. Granskningen innebär att en översyn av personuppgiftsbiträdesavtal samt incidenthantering behöver göras.

## 2.4 Övriga riskanalyser och egenkontroll

Ett antal mindre omfattande informationsklassningar och riskanalyser har genomförts under året för olika tjänster och system som t ex dialysbehandling i hemmet, akutrum med läkare på distans, IT-stöd för cytostatikabehandling. Efterfrågan om stöd gällande dessa frågor ökar från verksamheterna, vilket i sig är positivt, men kan vara svårt att hinna med.

## 2.5 IT säkerhet

Egenkontroll har genomförts gällande användningen av höga behörigheter i Region Jämtland Härjedalens Active Directory (AD). Målsättningen med kontrollen är att identifiera de fall där konton tilldelats för höga behörigheter i relation till kontots tilltänkta användningsområde. Kontrollen har gett underlag för korrigerande åtgärder.

Vidare har kontroll av IT driftsleverantörens hantering av månatliga säkerhetsuppdateringar gjorts. Brister i hanteringen noterades samt en försämring på serversidan i samband med semestertider. Detta är påtalat för IT drifts leverantören.

## 2.6 Skydd mot olovlig åtkomst - loggkontroller

Regelverket för utförande av systematiska och riktade loggkontroller i vårdsystem (främst Cosmic) uppdaterades 2016. Loggkontroller ska utföras var 3:e månad i verksamheterna. Ingen central uppföljning avseende utförda loggkontroller har genomförts för 2017. Fokus har istället varit utveckling och implementering av logg verktyget Logpoint (se 3.8)

Kommande år är det lämpligt att utföra både uppföljning av loggkontroller samt uppföljning avseende hur logg verktyget uppfyller användarnas krav.

## 2.7 Revision HSA och SITHS

Under 2017 har Inera genomfört en extern revision avseende Region Jämtland Härjedalens hantering av HSA samt SITHS. Den externa revisionen visar för **hanteringen av HSA-katalogen** att:

det finns brister i aktualiteten hos HSA-uppgifterna om regionens medarbetare. Främsta orsaken till detta är att uppföljning och registervård inte sker i tillräcklig omfattning.

Samma revision visar för **hanteringen av SITHS-korten** att:

det finns brister i efterlevnad av rutiner för identifiering av medarbetare vid utlämning av kort samt vid registreringen av utlämnade kort. Det finns även brister i hur certifikat spärras när medarbetare avslutar anställning/uppdrag och kortet ska spärras (återlämnas).

För att förbättra hanteringen har åtgärdsplaneringar tagits fram för ovanstående punkter. En förändring som skett under 2017 är att mer SITHS administration centraliserats genom att det har förts över till det nya funktionen Servicecenter vilket bedöms vara positivt, då det i en decentraliserad hantering är svårare att upprätthålla kvalitén.

## 2.8 Avvikelser och incidenter

Antalet rapporterade avvikelser som klassificerats som informationssäkerhet har en minskande trend för 2016-17 jämfört med åren dessförinnan. Orsaken till detta bedöms i första hand bero på en underrapportering som beror på en fortsatt låg medvetenhet om denna typ av rapportering och vad den innebär. Det finns också okunskap kring vad som ska klassificeras som en informationssäkerhets avvikelse. I flera fall har också avvikelser felaktigt klassificerats inom informationssäkerhet när det istället handlar om bristande rutiner eller rutiner som inte följs inom t ex schemaläggning, journal- och remisshantering.

Några fall av dataintrång med obehörig läsning av patientjournal har rapporterats. Under 2017 har två polisanmälningar gjorts avseende dataintrång och två ytterligare utredningar pågår.

Händelser har också inträffat där lösenord har lämnats ut till användare i strid med gällande rutin för s.k. ”akutlösenord” då användaren saknar ett fungerande SITHS-kort för inloggningen. Sammanblandning av patients reservnummer och personnummer har också rapporterats i något fall vilket fått till följd att samma patients uppgifter registrerats på olika id-nummer vilken kan äventyra patientsäkerheten.

Under året har några oplanerade avbrott skett i Citrix och Cosmic, men inget har varat någon längre tid och eller gett några allvarliga konsekvenser för patientsäkerheten.

# 3 Genomförda förbättringar

## 3.1 Regelverk och utbildning

Ett flertal regelverk har tillförts ledningssystemet under året t ex:

- Regel för användningen av externa molntjänster inom regionen har tagits fram och trätt i kraft.
- förbättringar i auktorisationsprocessen har genomförts för att kunna säkra hur nya och uppdaterade IT-stöd införs inom regionen med särskilt uppdaterade del om externa molntjänster.
- Regelverk har tagits fram för hur mobila enheter ska hanteras via centralt styrd, standardiserad konfiguration.
- Mall för systemsäkerhetsplan har tagits fram till målgruppen systemägare.

Utbildningar för regionledning, chefer och registerkoordinatorer har genomförts för hur personuppgifter får hanteras enligt EU:s kommande dataskyddsförordning (GDPR). En

kommande e-utbildning i Saba Cloud för medarbetare i informationssäkerhet har också tagits fram och beräknas tas i drift under början av 2018.

## 3.2 Informationsklassning

Informationsklassning är som tidigare påtalats en viktig grund inom informationssäkerhetsarbetet. Begreppet innebär att informationens värde fastställs utifrån de fyra perspektiven konfidentialitet, riktighet, tillgänglighet och spårbarhet. Syftet med att klassa information är att identifiera rätt säkerhets- och skyddsnivå för information som hanteras i samhällsviktiga och verksamhetskritiska processer. Informationens värde bedöms utifrån den funktion, känslighet och betydelse den har i verksamheten samt vilka konsekvenser det medför om det hanteras felaktigt, försvinner eller kommer i orätta händer.

För att löpande kunna utföra detta arbete krävs personella resurser, ett ramverk/modell för klassning, ett arbetssätt med roller och ansvar samt ett IT-stöd för att dokumentera och följa upp klassningen. Tidigare har Regionen arbetat med metoden BITS för systemklassning, dock var det ett fåtal system som var klassade. Det har sedan många år inte funnits någon förvaltning av BITS verktyget som var riktat mot säkerhet i system och inte för att klassa en informationsmängd i en process. Under 2015 lanserade Sveriges kommuner och landsting (SKL) verktyget KLASSA som hittills använts främst av kommuner. Regionens avsikt var att införa KLASSA som verktyg för informationsklassning under 2017. Efter ytterligare utvärdering av verktyget så anser dock Regionen inte att det är ett tillräckligt bra, nationellt är det också främst kommuner som valt att använda KLASSA. KLASSA är, liksom BITS, mest riktat mot att klassa system och inte informationsmängder. Det finns inte någon möjlighet att beskriva varför vissa klassningsnivåer har valts samt vilka konsekvenser eller påverkan som finns som grund för klassningen. Slutligen är verktyget är inte särskilt anpassat till vård (t ex krav från patientdatalagen) vilket gör att de kraven och tillhörande åtgärderna inte omfattas i klassningen. Därav har omtag fått göras i frågan om informationsklassning.

Regionen har utvecklat en egen mall för att manuellt kunna genomföra klassning, vilket också har gjorts ett flertal gånger under året. Det fungerar tillräckligt bra för att klassa olika typer av information och t ex kunna göra en kravställning inför upphandling och införande av nya tjänster eller system. Dock är den bristfällig för att klassa IT system och över tid kunna arbeta med åtgärdsplanering och systemsäkerhet. För att kunna arbeta strukturerat och löpande med systemförvaltning av befintliga system och i verksamhetsprocesser där informationen används krävs ett IT verktyg som stöd. Avgörande för att kunna uppnå ett strukturerat arbete med värdering och skydd är också att rollen informationsägare finns utpekad, vilket ytterligare behöver förtydligas i Regionen. Detta krävs för att kunna få ett tydligt ansvarstagande för hur informationen ska värderas och därmed skyddas.

Under året har ytterligare omvärldsbevakning gjorts och det har visat sig att många landsting har, liksom vi, utarbetat egna metoder som hanteras manuellt. Ytterligare ett IT-stöd (verktyg) för klassning har också utvärderats. Myndigheten för samhällsskydd och beredskap ska inom kort publicera ett metodstöd som ger tillämpad hjälp att klassa information och att arbeta med förbättringsåtgärder. Regionen avvaktar resultatet av det arbetet innan vidare beslut tas. Förhoppningsvis kan val och införskaffande av

klassningsverktyg göras under 2018. Fram tills att vi hittat ett metodstöd och verktyg som fungerar får den egenutvecklade mallen användas.

## 3.3 IT-säkerhet

Bland de förbättringar som genomförts under funktionsområdet IT-säkerhet kan nämnas förbättrad hantering av uppdateringar för servermiljön. Dessutom har ett fortsatt arbete avseende förbättrad nätarkitektur genomförts.

Det har gjorts en gallring av tjänstekonton och administratörskonton med för höga behörigheter i Region Jämtland Härjedalens domän. Åtgärden är vital för att minska regionens riskexponering men är samtidigt bara ett första steg i ett mer omfattande arbete för att säkerställa kontroll över hanteringen av höga behörigheter i Regionens IT-infrastruktur. Därav är ett arbete påbörjat med att ta fram ett koncept som säkerställer såväl kontroll över hanteringen av höga behörigheter men också som minskar risken för att konton med höga behörigheter skall kunna nyttjas av angripare i Regionens IT-infrastruktur.

Rutiner för skadlig kod har utarbetats och två potentiella utbrott av Ransomware (utpressningsförsök) har förebyggts genom skräddarsydda motmedel. Rutin för akut lösenordshantering (på jourtid) som uppstår när användare har glömt eller förlorat sitt SITHS kort har uppdaterats. Rutinen är skickad på remiss och därmed ännu inte beslutad. Det sker också ett pågående arbetet med skyddsåtgärder kopplat till införande av Office 365.

## 3.4 Införandeprojekt Garbo – en anpassning inför nya Dataskyddsförordningen

Dataskyddsförordningen införs som lag i hela EU från mitten av 2018 och ersätter och skärper skrivningarna i personuppgiftslagen (PuL). Förordningen förtydligar den personuppgiftsansvariges ansvar och skyldigheter. Anpassningen handlar översiktligt om att skapa medvetenhet i organisation och hos beslutsfattare, att skapa kontroll över i vilka sammanhang personuppgifter lagras, hur processerna ser ut för hanteringen samt att rätt dokumentation finns. Redan i december 2016 gjordes en förstudie och under våren 2017 togs beslut om att starta ett införandeprojekt med extern projektledare. Projektet som startade i september 2017 och som sedan kom att benämnas ”Garbo” har löpt på under hösten. Beredskapschef är projektägare och Regionledningen är styrgrupp.

Regionstyrelsen har ansvar för övergripande samordning av personuppgiftsbehandlingen och regionstaben har administrativt samordningsansvar. Däremot ligger det formella juridiska ansvaret på respektive nämnd som därmed även har ansvaret för personuppgiftsbiträdesavtal samt för underbiträden. Den nya rollen Dataskyddsombud är obligatorisk att utse av personuppgiftsansvarig (styrelsen) enligt förordningen. Denna roll har bland annat till uppgift att föra förteckningar över behandlingar av personuppgifter. Inom projektet kommer våren 2018 förslag att utarbetas för hur Dataskyddsombudets roll ska fungera i Regionen samt hur ansvaret för personuppgiftshanteringen ska fördelas.

Projektet ska vidare tydliggöra kravställning och genomföra kopplade åtgärder för att säkra att lagkraven i den nya förordningen kan efterlevas i regionens verksamheter. Åtgärder som avses är både av organisatorisk, processinriktad och teknisk art. Några av projektets effektmål är att kraven i Dataskyddsförordningen ska vara identifierade och kommunicerade till ansvariga i organisationen och att nödvändiga förändringar inom regionen gällande DSF är genomförda eller planerade. Det är inte rimligt att tro att alla nödvändiga åtgärder kan vidtas innan maj 2018, men det ska finnas planering och förslag. Efter det vidtar också ett prioriteringsarbete, då flera åtgärder kan komma att kosta pengar t ex avseende anpassningar av IT system. Ett annat viktigt effektmål är att allmänheten ska ha fortsatt förtroende för regionens hantering av personuppgifter och att Regionen undviker sanktionsavgifter och skadestånd.

Ett grundarbete inom projektet har varit att inventera Regionens personuppgiftsbehandlingar en s.k. registerinventering. Ett IT stöd är införskaffat för registreringen, det kan beskrivas som ett register över våra register. Ett omfattande arbete återstår också med att kvalitetsgranska de gjorda registreringarna, vilket inte har varit möjligt att avsätta resurser till under hösten.

En s.k. GAP analys har genomförts, i syfte att se vad som återstår för att Regionen ska leva upp till de nya lagkraven. En aktivitets- och åtgärdsplan skapas nu med de viktigaste områden och aktiviteterna för att skapa struktur för vårens arbete. Prioriterade arbeten kommer bl.a. att vara information till registrerade, översyn av personuppgiftsbiträdesavtal samt riskanalyser för extra känsliga personuppgifter. Riktat arbete kommer att ske mot Personalavdelningen som har omfattande inslag av personuppgiftshantering i sin verksamhet. Projektet kommer att avslutas 2018-05-31.

## 3.5 COSMIC

COSMIC uppgraderades till ny version (R8.1) helgen 13-14 maj 2018. Uppgraderingen gjordes från lördag 13 maj kl 03.30 till söndag 14 maj kl 10.00 och förde med sig ett driftstopp på drygt 36 timmar. Uppgraderingen gällde helt ny läkemedelsmodul, nytt gränssnitt (utseende) och nya översikter, och var en del i en större uppgradering som gjordes för samtliga COSMIC-kunder i ett kundgemensamt införandeprojekt. I och med uppgraderingen tillfördes utökad verksamhetskritisk funktionalitet och en ny teknisk plattform, nödvändig för ytterligare framtida förbättringar av COSMIC. Under driftstoppet arbetade verksamheten enligt reservrutiner: dokumentationer på papper, vilka överfördes till COSMIC efter driftstoppet, och därefter makulerades (undantaget uppgifter som skannades för spårbarhet).

Inför driftstoppet gjordes en omfattande genomgång av centrala reservrutiner vid driftstopp av COSMIC, som en del av kontinuitetsplaneringen. Rutinerna arbetades fram i ett tvärprofessionellt och organisationsövergripande samarbete. Arbetet resulterade i en checklista för reservrutiner, reservrutiner för journal, läkemedel, remiss, laboratoriemedicin, röntgen och fysiologi, hantering av blodprodukter och EKG. Förutom de rutiner som kompletterade de centrala rutinerna per klinik, uppgraderades även rutiner för IVA, Operation och Akutmottagningen. Eftersom reservrutinerna till en del gällde vid ett

specifikt tillfälle (aktuellt driftstopp) omarbetades sedan rutinerna till att gälla både oplanerade och planerade driftstopp, under slutet av 2017. Reservrutinerna är publicerade med länk från Insidan och COSMIC-fliken under Reservrutiner vid driftstopp.

Arbetet med att anpassa behörigheter, så att användare inte kan se eller göra för mycket eller för lite, har fortsatt under 2017. Fokus har framförallt varit att anpassa för de medarbetare som inte har en vårdrelation, men som utför arbetsuppgifter som innebär att de behöver åtkomst till vissa uppgifter i COSMIC. Exempel på vidtagna förbättringar är t ex för personal på beställningscentralen som ska kunna läsa sjukreseintyg och patienters adress. Där har begränsningar införts så att de endast har tillgång till det som krävs för att kunna utföra arbetsuppgiften. Anpassningar har även gjorts för den personal som ska ta emot samtal till den privata HC Ripan. För studerande i Regionen (alla yrkeskategorier) har behörighet förberetts så att den studerande tvingande behöver ange vidimerare av journal.

Handboken för behörighetstilldelning har omarbetats för att underlätta översikt, och ge utrymme för behov som finns per klinik genom riktad information. Dessutom har tilldelningen av behörigheter satts ihop i ”paket” för att underlätta för lokala COSMIC-administratörer. Två (likadana) utbildningstillfällen har anordnats för detta. Arbetet med behörighetsstyrning och tilldelning kommer att fortsätta under 2018. Det behövs också ett klargörande avseende hur beslut om behörigheter ska tas och hur de ska följas upp.

## 3.6 Journal på nätet

Regionstyrelsen har beslutat att journal via nätet skulle införas för medborgare i Jämtland/Härjedalen under 2017. För tjänsten fanns ett nationellt regelverk med bindande krav och vissa valfria delar. Under första halvåret av 2017 utformades regelverk samt vilka delar av journalen som ska finnas tillgänglig. Regionen har valt att bl.a. visa Anteckningar, Vårdkontakter, Diagnoser, Läkemedel, Klinisk kemi och Röntgensvar.

En arbetsgrupp har tillsatts som löpande har arbetat med införandet. Strax innan jul blev det klart att Region Jämtland Härjedalen blivit godkända av Inera för driftsättning av journalen den 15:e januari.

En central support har inrättats för att kunna hantera invånarärenden gällande journalen via nätet. Ett rutindokument och blanketter har tagits fram för att kunna hantera förseglingar och hävningar av försegling av direktåtkomst för invånare till journalen. Arbete pågår också för fullt med att lösa frågan om att akut kunna försegla invånares direktåtkomst på vårdens begäran. Barnskyddsteamet är kontaktat och dialog pågår. Det har hållits tre informationstillfällen i hörsalen och ytterligare ett kommer att hållas i januari.

Arbetet kommer att flyttas över ifrån projektgrupp till förvaltning under våren 2018.

## 3.7 Nya rutiner för ID kontroller

Frågan om rutiner för ID kontroller aktualiserades inför införande av det nya arbetssättet med självincheckning på Specialistvården. Det har också förekommit avvikelser i vården där patienter uppgivit falsk identitet. Frågan är viktig både ur patientsäkerhet- och informationssäkerhetsaspekter. Ett uppdrag gavs från Regionala säkerhetsrådet till verksamhetschef för patientsäkerhet och Beredskapschef att göra en översyn av befintliga rutiner samt föreslå nödvändiga förbättringsåtgärder. Uppdraget har genomförts med revidering av rutiner för ID kontroller med förtydligande att det är obligatoriskt att utföra. Anpassningar har också gjorts i Cosmics mallar för nybesök. I COSMIC finns ett sökord för legitimationssätt, vilket också gör att man kan följa upp om legitimationskontroll utförts. Stickprov som är gjorda under hösten visar att användningen ökat på totalen, även om det skiljer sig åt mellan olika mottagningar. Inför att de nya rutinerna togs i bruk, så gjordes en informationsinsats både till medarbetare och patienter.

## 3.8 Roller och ansvar COSMIC samt nationella eHälso-tjänster

Att arbeta med förtydligande av ansvar och roller gällande IT- och informationssäkerhetsfrågor i COSMIC prioriterades i både Regionstyrelsens samt Regiondirektörens verksamhetsplaner för 2016. Arbetet fick dock flytta över till 2017 och under våren genomfördes en workshop med berörda verksamheter representerade. Syftet med workshopen var att tydliggöra vilka frågor och områden det handlar om samt att beskriva befintliga strukturer. Vidare var också syftet att diskutera huruvida det finns rätt strukturer och samverkansarenor för att kunna arbeta effektivt. Då området också tangerar mobila tjänster för vård och behandling, ett område som utvecklats snabbt de senaste åren, bjöds företrädare in även för detta område.

Resultatet av workshopen var sammanfattningsvis att det pågår enormt mycket arbete, men ofta i helt separerade spår. Det tydliggjordes att flera av omnämnda områden har ett ömsesidigt beroende av varandra, det finns många gemensamma intressen och flertalet av pågående arbeten påverkar både informations- och IT säkerhetsarbetet. En gemensam nämnare var också att företrädare för de båda säkerhetsområdena ofta kommer in sent i processerna, vilket skapar stress men också bidrar till att säkerhetsföreträdarna upplevs som ”bromsklossar”. Det finns ett tydligt behov av att skapa transparens mellan olika områden och hitta gemensamma arenor så att arbetet flyter bättre. Alla var också överens om att utveckling inte ska förhindras, men att säkerhetsarbetet ska vara en del i utvecklingsarbetet.

Det visade sig också att det finns oerhört många mötesforum, men egentligen inget där de olika företrädarna möts. Det finns också en rädsla att resultatet av workshopen ska skapa ännu fler möten, vilket ingen är intresserad av då de flesta upplever hög arbetsbelastning av många möten.

Resultatet av workshopen ska presenteras för Regionledningen. Ett förbättringsförslag är att ett antal av informationssäkerhetsrådets möten (t ex 3-4/år) utökas med företrädare för COSMIC och eventuellt för nationella E-hälsotjänster. Syftet är då att skapa transparens och få kännedom om varandras pågående och kommande arbeten samt även att dessa företrädare kan förbereda och lyfta upp säkerhetsfrågor till detta forum. Ett annat forum som kan utvecklas är också det befintliga Regionala säkerhetsrådet, där det aldrig hanteras

några COSMIC frågor, fast det är en viktig patientsäkerhetsfråga. Förslag uppkom också om att företrädare för samordning av säkerhet bjuds in till något av de befintliga forum som finns inom förvaltning av COSMIC- och eHälsoområdet.

Andra saker som framkom var att det finns oklarheter gällande vem som egentligen ansvarar för vad och vem som har beslutanderätt i vissa frågor. Detta bidrar till att frågor dras i långbänk eller i värsta fall stannar av. Det är också viktigt att olika styrdokument för e-hälsa, mobila tjänster, COSMIC förvaltning finns tillgängliga och sökbara för att kunna eftersöka information och skapa transparens. Generellt finns behov av ett mer processinriktat arbetssätt för IT- och informationssäkerhetsfrågor.

## 3.9 Loggkontroller vårdadministrativa system

Under året har ett systemstöd (Logpoint) för systematisk loggkontroll införts i samtliga vårdverksamheter inom Östersunds sjukhus. Under 2018 införs motsvarande arbetssätt i primärvården. Arbetssättet ger möjligheter till bättre uppföljning av medarbetares åtkomster till patientuppgifter i det vårdadministrativa systemet COSMIC.

Detta är en del i det förebyggande och uppföljande skyddet för patienternas integritet. Kontroller utförs både som stickprov och löpande för att säkerställa att regelverket efterlevs.

# 4 Prioriterade åtgärder 2018 - 2019

Följande åtgärdsområden finns med i den övergripande handlingsplanen för informationssäkerhet 2018-2019;

1. Säkerställa lagefterlevnad för personuppgiftsbehandlingar
2. Tillhandahålla ett strukturerat beslutsunderlag till ledningens genomgång
3. Tillhandahålla utbildning och stöd för medarbetare samt riktad utbildning till nyckelfunktioner såsom chefer, systemägare/systemansvariga och informationssäkerhetsombud
4. Etablera systematisk kontinuitetshantering för verksamhetskritiska
5. informationssystem
6. Etablera en ändamålsenlig internkontroll för informationssäkerhet
7. Etablera ett riskbaserat arbetssätt inom informationssäkerhet
8. Tydliggöra och kravställa säkerhetsrelaterade uppgifter i systemförvaltningen

Varje åtgärdsområde har ett antal aktiviteter som fördelats ut i förvaltningarna. På aktivitetsnivå innebär det t ex att Hälso- och sjukvårdsförvaltningen samt regionstaben ska informationsklassa och riskanalysera sex utvalda kritiska IT-system. Kopplat till det ska också översyn göras huruvida ändamålsenliga reservrutiner finns. Informationssäkerhetssamordnarens uppgift blir här att stödja systemansvariga samt följa upp arbetet. Det finns också aktiviteter kopplat till personuppgiftsbehandlingen och projektet Garbo.

Det finns också en ambition att utarbeta ett ramverk för hur riskhantering inom informationssäkerhet ska hanteras samt hur uppföljning och lärande från rapporterade avvikelser ska göras och kopplas till det riskförebyggande arbetet.

Uppföljning av loggkontroller i Hälso- och sjukvården ska ske under 2018.

Regionens policy för informationssäkerhet behöver också revideras under 2018.