REGION JÄMTLAND HÄRJEDALEN

Informationssäkerhetsberättelse 2016

Version: 1

Beslutsinstans: Regionstyrelsen

ÄNDRINGSFÖRTECKNING

Version	Datum	Ändring	Beslutat av
1.		Nyutgåva	Regionstyrelsen

INNEHÅLLSFÖRTECKNING

1 INFORMATIONSSÄKERHETSARBETE 2016

Enligt SOSFS 2008:14 ska vårdgivaren utse en eller flera personer som ska ansvara för informationssäkerhetsarbetet. 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 informationssäkerhetsarbetet har gått framåt så går utvecklingen inom IT området snabbt och de tekniska möjligheterna ökar för all verksamhet inom Regionen. Verksamheterna idag har ett högt IT beroende och därmed ökar riskerna och sårbarheterna. Avdelade resurser för informationssäkerhetsarbetet har inte motsvarat behovet, alla mål har inte uppnåtts och alla planerade aktiviteter har inte genomförts. Regionen står inför stora utmaningar när det gäller att leva upp till kraven i den nya Dataskyddsförordningen och att skydda vår information. Det arbete som pågått under flera år har tappat fart under 2016 men positivt är att en informationssäkerhets-samordnare har rekryterats och beräknas börja sin anställning under första kvartalet 2017.

Ett prioriterat område inför 2016 var att etablera en organisation och ett IT stöd för loggkontroll, det arbetet har gått framåt och IT stödet beräknas successivt kunna bredd införas under 2017. Det mål som återfanns i både Regionstyrelsens och direktörens planering om behovet att klargöra ansvar och roller avseende informations- och IT

säkerhetsfrågor inom COSMIC förvaltning samt nationella E-hälsotjänster har inte genomförts. Planering finns för genomförande våren 2017. Regionfullmäktige fastställde i oktober en ny informationssäkerhetspolicy. Informationssäkerhet är nu en del i internrevision och ledningens genomgång vilket är mycket positivt både för strategiskt arbete samt dialog med verksamheter i våra förvaltningar. Kunskapsnivån i informationssäkerhet behöver höjas i verksamheterna och ett prioriterat område för 2017 är att införa en e-utbildning i informationssäkerhet.

1.1 Ledningssystem för informationssäkerhet (LIS)

Ledningssystem för informationssäkerhet (LIS) är en integrerad del av Region Jämtland Härjedalens ledningssystem. Informationssäkerhetsarbetet följer standarden ISO 27001. Kontinuerligt arbete krävs för att utveckla och hålla ledningssystemet aktuellt. 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.) avseende att säkerställa en korrekt personuppgiftshantering. Vidare behöver regelverk kring användning av molntjänster utvecklas. Ett ökat fokus behöver läggas på att ge chefer större möjligheter att tilldela och följa upp behörigheter för sin personal. Det finns också behov av ökad kunskap i alla verksamheter om informationssäkerhet. Avsaknad av digital utbildning inom informationssäkerhet är en sårbarhet i Region Jämtland Härjedalen.

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 ett steg i rätt riktning. Frågan om översyn av systemförvaltningsmodell har lyfts upp och finns i verksamhetsplaneringen för 2017. Beslut har tagits om att Id kontroller vid sjukvårdande behandling bör utredas och att relevanta rutiner upprättas. Regionledningen ser fördelar med att byta till KLASSA som systemklassningsmodell och har gett Beredskapschef i uppdrag att bereda ett beslutsunderlag.

1.3 Handlingsplan informationssäkerhet

Handlingsplanen för 2016-2017 (RS/1444/2015) har reviderats och fastställts av Regiondirektören. Kompletteringar avseende registerinventering har gjorts, vilket är ett viktigt steg i förberedelsearbetet inför Dataskyddsförordningen. En regionövergripande handlingsplan inom området fyller fortfarande ett viktigt syfte som styrdokument inom ett eftersatt och svårstyrt område.

2 RISKANALYSER OCH EGENKONTROLL

2.1 Övergripande risk- och behovsanalys behörigheter COSMIC

Riskanalys som genomförts avseende behörigheter i COSMIC slutfördes i juni 2016 och överlämnades till Objektsägaren för COSMIC d.v.s. hälso- och sjukvårds-direktören. Analysen visar att det finns risker inom

behörighetsprocessen, både inom tilldelning och uppföljning av behörigheter. Det finns också risker främst kopplat till för vida behörigheter. Åtgärdsförslag är bl.a. att det införs användarroller och att en viss begräsning införs i hur mycket information en användare kan se utan att göra aktiva val. Översyn bör ske om det kan införas säkerhetsåtgärder för särskilt skyddsvärda patienter och enheter. Åtgärder har påbörjats inom COSMIC förvaltning utifrån analysens förslag.

2.2 Övriga riskanalyser och egenkontroll

Några riskanalyser har genomförts bl.a. inom psykiatrins öppenvård avseende införande av sms utskick, inom barn gällande införande av BVC modul i journalsystemet samt hos patientnämnden avseende VISMA vårdsynpunkter.

IT chefen fick inför 2016 ett uppdrag att se över systemförvaltningsmodell för Region Jämtland Härjedalen. Arbetet har dock prioriterats bort under 2016 men ska genomföras 2017. I det arbetet är det sedan tidigare fastställt att de risker, brister samt förbättringsförslag som framkom i tidigare genomförd riskanalys avseende systemförvaltning ska beaktas.

Checklistan i ledningssystemet för egenkontroll av det systematiska kvalitetsarbetet har kompletterats med delar om informationssäkerhet. I de internrevisioner som har genomförts under 2016 har frågor ställts angående kontinuitetsplanering, ansvars och utbildningsfrågor samt loggkontroller. Resultatet av internrevisioner visar bl.a. att det finns brister i verksamheten avseende kontinuitetsplanering i ett flertal verksamheter och flera verksamheter efterlyser utbildning i

informationssäkerhet. När det gäller loggning i vårdadministrativa system visar internrevisionen att kunskapen om loggkontroller är relativt god, loggkontroller hade genomförts i nio av tio verksamheter. Uppföljning har gjorts mot den verksamhet som inte gjort loggkontroller och de har nu rättat till bristen.

2.3 Granskning av IT-säkerheten/Informationssäkerheten

Revisionskontoret har genomfört en förstudie i syfte att kartlägga och bedöma om det finns anledning för förtroendevalda revisorer att besluta om en fördjupad granskning. Bedömningen är att det pågår ett aktivt arbete för att säkerställa informationssäkerheten och går därmed inte vidare med någon fördjupad granskning. De konstaterar att det finns en mängd kända brister av varierande allvarlighetsgrad och att de åtgärder som vidtas löpande inte sker i tillräcklig takt. I rapporten lyfts några angelägna förbättringsområden fram där Regionstyrelsen ska redovisa vilka åtgärder som planeras att vidtas senast 31/3 2017. De förbättringsområden som nämns är främst inom informationsklassning, systemförvaltning, uppföljning av standarden ISO 27001, användarkunskaper hos medarbetare samt att resurser för nödvändiga åtgärder säkerställs och tydliggörs.

2.4 SITHS förvaltning och revision

Under året har interna revisioner men ingen extern revision genomförts för SITHS förvaltning (utgivning och hantering av SITHS-etjänstekort och certifikat). Granskade områden för de interna revisionerna har varit rutiner för distributionskedjan för SITHS-kort till lokala utlämningsställen i länet samt rutiner för själva utlämningsställena (lokala SITHS-administratörer).

Resultatet av revisionerna visar att:

1) För kortdistributionen till länets hälsocentraler (via transportenhetens slingbilar) sköts detta med mycket bra efterlevnad av gällande rutiner. Utförande personal är väl insatta i rutinerna och har tydliga rutiner för hur förmedling, förvaring och kvittenser av kort ska ske.
2) För utlämning av kort på granskade hälsocentraler finns vissa avvikelser i efterlevnaden av gällande regler. Särskilt gäller detta att dubblettkort i flera fall har lämnats ut till användare, något som inte får förekomma. Detta innebär att fler än ett aktivt kort tilldelas en användare vilket strider mot reglerna för SITHS. En användare får endast inneha ett aktivt kort åt gången. Åtgärder för att komma till rätta med denna typ av avvikelse är att informera berörda lokala SITHS-administratörer om gällande regler.

Fortfarande förekommer enheter/avdelningar inom Östersunds sjukhus där en låg volym av SITHS reservkort ges ut till den egna enhetens/avdelningens personal vilket riskerar att sänka kvalitén på hanteringen. Planen är att det Servicecenter som under 2017 ska etableras som ett stöd för verksamheterna ska hantera beställning och utlämning av SITHS-korten lokalt inom Östersunds sjukhus. Därmed försvinner behovet av att ha lokala SITHS-administratörer som hanterar reservkort inom varje område/enhet på sjukhuset.

2.5 Ny Dataskyddsförordning

En ny lagstiftning, EU:s Dataskyddsförordning, ersätter personuppgiftslagen fullt ut from maj 2018. Översyn av konsekvenser för den nya Dataskyddsförordningen pågår. Detta inkluderar en översyn av

organisation avseende personuppgiftshanteringen och förslag för organisation av personuppgiftsombud (PuO). Den nya lagen ställer bl.a. krav på att Regionen alltid vet vart vårt data/information befinner sig och vilka som har behörighet till den. Det kräver en kartläggning av våra informationsflöden. Regionen behöver också ha kontroll över vem som gjorde var och när d.v.s. en mycket mer omfattande loggning än vad vi har idag. Till lagstiftningen har kopplats viten. Datainspektionen kan komma att utdöma en sanktionsavgift om verksamheten bryter mot förordningens regler. Avgiften bedöms utifrån hur allvarlig överträdelsen är, om det skett avsiktligt eller inte, vilka åtgärder man har vidtagit för att minska skadan, om man tjänat ekonomiskt på överträdelsen och andra försvårande eller förmildrande omständigheter.

För att skapa överblick över vilka personuppgiftsbehandlingar som utförs i Region Jämtland Härjedalen har en aktivitet lagts till i handlingsplanen för 2017. Samtliga avdelningar och områden ska under 2017 rapportera in i vilka system och register man hanterar personuppgifter. Regionen behöver alltså ”skapa ett register över sina register”. Det finns idag ingen exakt beräkning för vad det kommer att kosta för att möta kraven i den nya förordningen. En nödvändig initial åtgärd är att alla våra verksamhetssystem informationsklassas och kartläggs bl.a. utifrån hur de uppfyller kraven. Ett ansvar som vilar på systemägarna.

2.6 Avvikelser och incidenter

Sammanlagt finns 64 avvikelser registrerade vilket är en minskning jämfört med tidigare år. 31 avvikelser berör IT system och IT säkerhet (se IT säkerhetsincidenter), antalet avvikelser som gäller COSMIC har minskat jämfört med 2015 då systemet infördes. 20 avvikelser är

klassificerade inom sekretess. Flera av dessa handlar om att dokumentation t ex patientliggare lämnats kvar i skrivare eller ute i vårdverksamhet, att felaktigt patient tid använts på intyg, provrör m.m. Några avvikelser är kopplat till felaktiga SMS påminnelser gått ut. En avvikelse finns registrerad angående att post rutinen inte följts för patienter med skyddad identitet. En polisanmälan har gjorts avseende dataintrång/sekretessbrott och en polisanmälan har gjorts avseende bedrägeri, där försök gjorts att stjäla annan persons identitet. Fortfarande finns kvalitetsbrister i rapportering och klassificering av avvikelser inom informationssäkerhet. Ett arbete har gjorts inom Centuri avvikelsesystem för att förändra och förenkla avvikelseformuläret, men det har ännu inte tagits i drift.

I juni inträffade ett driftsavbrott i COSMIC där TiB tog beslut om allvarlig händelse. Uppföljning har gjorts för översyn av larm och kommunikationsvägar. Ingen patient kom till skada.

2.6.1 IT säkerhetsincidenter

En incidenttyp som blivit ytterligare mer frekvent jämfört med tidigare är angrepp av ”ransomware” (skadlig kod som låser/raderar filer) En lösensumma begärs för att göra filerna läsbara igen. Angreppen har skapat merarbete i form av återskapande av filer från säkerhetskopior och det kan inte uteslutas att förlust av information/filer också har skett i vissa av fallen. Under året har också ett par kortare driftstörningar skett för COSMIC vårdadministrativt system. En allvarlig händelse var också en inträffad driftstörning på kopplingen som förmedlar elektroniska remisser i röntgensystemet (RIS) vilken innebar att ett par remisser raderats, något som dock har upptäckts i efterhand. Kortare avbrott har också

inträffat i regionens funktion för fjärranslutning till IT-miljön (VPN-koppling), något som medfört att det inte gått att nå IT-systemen från distansarbetsplatser.

En tydlig trend under året är det alltmer ökade hotet från skadlig kod som angriper IT-system och filer. Detta hot behöver löpande mötas med allt effektivare skyddsåtgärder för att inte riskera allvarliga driftstörningar och informationsförluster. Det är väsentligt att införande av skydd mot detta ökade hot kan få utökade resurser/finansiering eftersom bristande skydd kan medföra stora kostnader och även betydande patientsäkerhetsrisker. En prioriterad åtgärd är också användarutbildning då användarnas beteende kan påverka vilka risker vi utsätts för.

3 GENOMFÖRDA FÖRBÄTTRINGAR

3.1 Regelverk informationssäkerhet och utbildning

Under året har ett flertal nya regler och rutiner utarbetats. Dokumentet ansvar för informationssäkerhet har reviderats. Regler och rutiner för loggkontroll har uppdaterats samt att organisation och ansvar för loggkontroll nu finns beskrivet. För att ge stöd till chefer har ett dokument avseende offentlighet och sekretess utarbetats, vilket även innefattar utlämnande av allmän handling.

Två workshops med extern worshopledare har genomförts i syfte att uppnå ett förbättrat arbetssätt i informationssäkerhetsarbetet. Fokus har framförallt varit informationsklassning, införandet av ledningssystem för informationssäkerhet samt upplägg av utbildning för

informationssäkerhet. En genomgång av styrkor och svagheter inom området har också gjorts.

Utbildning har genomförts för verksamhetschefer inom juridik t.ex. offentlighet- och sekretesslagen, patientdatalagen samt kraven i socialstyrelsens föreskrifter om informationshantering och journalföring. Utbildningsinsatser har också genomförts för Regionfullmäktige och Regionstyrelsen. Sedan 2016 ingår också sekretess och informationssäkerhet på introduktion för nyanställda som genomförs både vår och höst.

3.2 IT säkerhet

Bland de förbättringar som genomförts inom funktionsområdet IT-säkerhet finns:

- Klientsäkerheten har löpande höjts utifrån en åtgärdsplan för skydd mot den alltmer ökande typen av skadlig kod, s.k. ”ransomware” (gisslanprogram som låser/raderar filer och begär lösensumma)
- Påbörjat införandet av en förbättrad nätarkitektur med utökad segmentering av olika nätdelar utifrån säkerhetskrav på hur kommunikation får ske inom nätet
- Kravställt på förbättrat skydd mot skadlig kod i form av s.k. ”vitlistningsskydd”
- Tagit fram en första version av modell/krav för hantering av mobila klienter (läsplattor och smartphones)
- Genomfört en intern revision av hanteringen av driftkonton inkl. s.k. privilegierade behörigheter i regionens IT-miljö

- Förbättrat kraven på loggning av händelser i regionens IT-infrastruktur
- Påbörjat arbete med förbättringar i säkerhet för fastighetsnätet och dess kritiska driftsfunktioner för bl a klimatförsörjning och styrning av övervakning mm
- Genomfört riskanalyser av flera olika områden inom IT-infrastrukturen (server, nät- och klientmiljöer)
- Tagit fram förenklade åtgärdsmallar för hur system ska hanteras för olika säkerhetsnivåer (aspekten' tillgänglighet')

3.3 COSMIC

Under 2016 har översyn och justering påbörjats avseende vilken information i COSMIC olika användare ska ha tillgång till, med start av användare som utför administrativa arbetsuppgifter, grundat på arbetsflöden att utföra tilldelad uppgift.

Användarrollen kvalitetsgranskare har införts i COSMIC inklusive beslut gällande hur hantering av tilldelande och avslutande av användarrollen ska ske, på lokal och central nivå. En handbok för behörigheter i COSMIC har publicerats.

Under 2017 kommer arbetet att fortsätta gällande behörigheter och vilken information i COSMIC olika användare behöver ha tillgång till. Det ska också säkerställas att rutiner för att lägga upp och avsluta behörigheter är väl kända och fungerar. Det ska också arbetas med framställande av centrala reservrutiner vid oplanerade driftsavbrott vad gäller vårddokumentation och läkemedel (ordination och administration av läkemedel).

3.4 Loggkontroller vårdadministrativa system

En prioriterad aktivitet för 2016 var att etablera organisation och införa IT stöd för loggkontroller i COSMIC. Loggkontroller består av två olika delar:

- Systematisk loggkontroll (löpande granskning med stickprov mm)
- Riktade kontroller (specifik granskning av åtkomster som är kopplade till extra skyddsvärd information)

IT stödet (Loggpoint) har införts, fortfarande återstår arbete med att anpassa systemet till behoven och att loggrapporter kan skapas med automatik d.v.s. att slumpvis utvalda användare ska kontrolleras i systematisk loggkontroll. I nuvarande skede krävs en del manuellt arbete, men det är fullt fungerande för att kunna köra loggar. En pilot test har genomförts på kirurgen och ett successivt införande beräknas göras under 2017. Internrevision visar att inte alla regelmässigt utfört loggkontroller enligt fastställda rutiner vilket är ett absolut krav och en viktig förtroende fråga.

3.5 Informationsklassning/BITS

Informationsklassning är 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.

Att BITS analysera ett IT system innebär i praktiken att göra en informationsklassning samt riskanalys och att ta fram åtgärdsförslag att skapa och upprätthålla systemsäkerhet. Under 2016 har BITS klassning och åtgärdsplanering genomförts för två verksamhetssystem Flexlab (labmedicin) och Prosang (blodcentralen). Under 2015 lanserade Sveriges kommuner och landsting (SKL) ett nytt verktyg som heter KLASSA som både kan användas för att klassa en informationsmängd och för att bedöma säkerheten i ett IT system. Ett försök har gjorts för att utvärdera och jämföra KLASSA med BITS samt den modell vi själva utarbetat för informationsklassning. Bedömningen är att KLASSA är ett enklare verktyg att använda för systemägare, det är också av vikt att det finns en förvaltning av KLASSA vilket det inte gör för BITS. Fortfarande har vi många system som inte är klassade och för verksamhetskritiska system behöver det arbetet ta fart under 2017. Förslag till beslut kommer att läggas fram till Regionledningen att systemklassning ska genomföras för verksamhetskritiska system och att KLASSA är det verktyg som rekommenderas.

3.6 Kontinuitetshantering

Ett framgångsrikt arbete har pågått över två år med att utarbeta och säkerställa reservrutiner för verksamheterna inom Akutområdet vid bortfall av verksamhetskritiska IT-system. Arbetet samt metod har återkopplats till övriga verksamhetschefer inom Hälso- och sjukvårdsförvaltningen och beslut har tagits att arbetet ska fortsätta inom andra verksamhetsområden. Parallellt kommer ett nytt arbete att startas upp i Akutområdet under 2017, med samma metod men inom område telefoni.

3.7 Övning driftsstörning IT

I mars 2016 genomfördes en övning för Särskild sjukvårdsledning baserat på ett scenario med omfattande driftsstörning i IT systemen samt IT infrastrukturen.

4 PRIORITERADE ÅTGÄRDER 2017

Handlingsplan informationssäkerhet finns utarbetad för 2016-2017 (dnr RS/1444/2015). Prioriterade områden och uppgifter är:

- Ansvarsfördelning ska tydliggöras för informations- och IT säkerhetsfrågor inom Cosmic förvaltning samt e-hälsotjänster.
- En inventering av regionens all personuppgiftshantering ska göras samt en översyn av organisation avseende personuppgiftsbehandling för att leva upp till kraven i den nya dataskyddsförordningen som 2018 ersätter nuvarande personuppgiftslagen (PUL).
- Utveckling av användarvänligheten av i loggverktyget Loggpoint. Systemet ska succesivt införas i verksamheten under 2017.
- Fortsatt arbete med kontinuitetshantering
- Molntjänster. Övergripande risk- och behovsanalys samt förbättring av regelverk för anskaffning av molntjänster.
- Klassning av verksamhetskritiska system med KLASSA som verktyg
- Planering för återstart och återställande av verksamhetskritiska system

- Införande av e-utbildning avseende informationssäkerhet
- Behörighetshantering. Högre grad av automatiserad behörighetsbeställning, ska också säkerställa styrning av behörigheter och ge chefer möjlighet att kontrollera behörigheter
- Säkerställa att kraven från EU:s nya dataskyddsförordning kan tillgodoses i regionens personuppgiftshantering/IT-system
- Förbättra säkerheten för mobila klienter/mobilt arbetssätt samt införa riktlinjer kring hantering och införande av mobila enheter
- Förbereda för anslutning till Sambi identitetsfederation för svensk vård och omsorg – för att underlätta informationsutbyte mellan olika huvudmän