Ett samlat svar om informationssäkerhetsarbetet vid RVN 2017 i enlighet med frågeställningar från patientsäkerhetsberättelsen:

Frågeställningar:
Uppföljning av informationssäkerheten, riskanalys avseende journalföring och behandling av personuppgifter, förbättringsåtgärder avseende informationssäkerheten, utvärdering av skyddet mot olovlig åtkomst till datornätverk och informationssystem samt granskning av att journalföring sker enligt gällande författning.

Svar:
I regionen sker den största delen arbetet med analyser, uppföljning och förbättringsåtgärder i förhållande till så kallad avvikelserapportering. Det arbetet påbörjades i mer strukturerad form runt Q1-2015 och har sedan dess kontinuerligt pågått i hela regionens verksamhet. Det är ett omfattande arbete och görs i enlighet med vetenskap och beprövad erfarenhet i förhållande till olika säkerhetsområden däribland informationssäkerhet. Det brister dock något när det gäller central uppföljning och sammanställning av informationssäkerhet, såväl när det gäller avvikelser som för området i övrigt.

Under året har 230 stycken avvikelser med direkt eller indirekt bäring på säkerhetsområdet informationssäkerhet registrerats i regionens avvikelsesystem. Registreringen i ett system innebär att varje enskild incident kommer att regleras på ett enhetligt och konsekvent sätt samt att spårbarheten säkras och ingenting riskerar glömmas bort.

Kontinuerligt informationssäkerhetsarbete bedrivs också inom alla systemförvaltningar och vid all systemutveckling. Som exempel på större riskanalyser under året inom utvecklings- och förvaltningsarbetet är bl.a. analyser vid införandet av nytt system för beställningar- och svar, BoS integrerat med basjournalsystemet NCS Cross samt flertalet analyser inför och under upphandling i det s.k. FVIS (Framtidens Vård Informations Stöd) projektet.

Som exempel på förbättringsåtgärder avseende informationssäkerheten kan nämnas framtagning av nya samt vidareutveckling av befintliga styrdokument på området. Under året har t.ex. regler kring identifiering av patienter samt anvisningar för post till adresskyddad och godkännande av leverantör av och tjänst för sociala medier

vidareutvecklats och en ny rutin vid flyttning och följande borttagning av felaktigt införd journaluppgift införts.

Inom ramen för ett samverkansavtal med regionens uppdragstagare för drift- och underhåll av vår IT-infrastruktur bedrivs ett regelbundet arbete inom ett så kallat Säkerhetsforum. Arbetet har främst IT-säkerhetsinriktning men hanterar också ofta frågor kring krav på ärendehantering och behörighetskontroller vid beställningar eftersom detta ofta utgör särskilda utmaningar i synnerhet i en outsourcad verksamhet. Under året har fyra dokumenterade möten hållits. 27 IT-incidenter har registrerats under året varav 1 mycket allvarlig, 8 allvarlig, 9 mindre allvarlig och 9 utan konsekvenser i enlighet med kategoriseringen beskriven nedan:

Kategori (nivå 1-4)

Klass 4 – Mycket allvarlig	Säkerhetsincidenter som har betydande konsekvenser för organisationen, till exempel koordinerade attacker, dataintrång, brand i datorhall eller stöd av känslig information. Mycket långa driftavbrott (>1 dag) för verksamhetskritiska system.
Klass 3 – Allvarlig	Säkerhetsincidenter som har konsekvenser för organisationen, till exempel datasabotage, konstaterande databedrägerier eller integritetsbrott. Hit hör också längre driftavbrott (<1 dag) för verksamhetskritiska system.
Klass 2 – Mindre allvarlig	Säkerhetsincidenter, till exempel försök till dataintrång, misslyckade attacker eller missbruk av IT-resurser. Andra exempel är längre driftavbrott (<0,5 dagar) för verksamhetskritiska system.
Klass 1 – Inga konsekvenser	Incidenter som hanteras av ordinarie verksamhet men som kan komma att eskalera till en säkerhetsincident, till exempel kortare driftavbrott, avsökningar, enstaka virus eller epostattacker. Till denna klass hör även mindre driftincidenter/avbrott.

I den årliga rapporteringen till MSB på indikatorer för bedömning av landstingets generella krisberedskap lämnades följande svar under punkten Informationssäkerhet:

1. Landstinget hanterar information säkert.

   - Landstinget bedriver ett systematiskt arbete med Informationssäkerhet i enlighet med tillämplig informationssäkerhetsstandard på området. Ja ☒ Nej ❑

   - Landstinget har rutiner för att identifiera och hantera kritiska beroenden till system och tjänster för informationshantering som är av central betydelse för landstingets verksamhet. Ja ☒ Nej ❑

Motivering: Vid landstingskansliets administrativa avdelning finns för närvarande fyra heltidstjänster som har till uppgift att helt eller till del stödja arbetet med informationssäkerhet. Informationssäkerhetssamordnaren, landstingets personuppgiftsombud, arkivarien samt en jurist. De arbetar samtliga systematiskt med såväl direkt verksamhetsstöd och uppföljning av detta som en kontinuerlig vidareutveckling av landstingets ledningssystem för informationssäkerhet, LIS.	Ja ☒	Nej ❑

2. Landstingen ställer krav på informationssäkerhet i förhållande till externa aktörer.

   - När informationshantering upphandlas av extern leverantör. Ja ☒ Nej ❑
   - När landstingsverksamhet bedrivs av extern leverantör Ja ☒ Nej ❑

Motivering: Vid respektive systemförvaltning bedrivs ett kontinuerligt riskanalysarbete inför behov av vidareutveckling och underhåll. Vid nyanskaffning av produkt eller tjänst säkerställs detta för närvarande i samverkan som en del av upphandlingsarbetet.	Ja ☒	Nej ❑

Nedan följer delar av årsberättelsen 2017 för Verksamhet Administration inom Regionledningsförvaltningen där tjänsten informationssäkerhetssamordnare samt rollen och tillikauppgiften personuppgiftsombud är organiserade:

Punkter från aktivitetsplanen:

- Under året har ett projekt startats upp inför den nya Dataskyddsförordningen GDPR, General Data Protection Regulation, som börjar gälla den 25 maj 2018. Projektet kommer bl.a. ta fram en handlingsplan för arbetet.

- En förbättrad digital registerförteckning är under uppbyggnad. Erfarenheter visar att skräddarsydda systemlösningar ännu så länge är onödigt komplexa och mer omfattande än våra behov och vår nuvarande förmåga. Vi bygger därför istället upp en enkel grund med en databas i MS Excel och lyfter successivt in data från olika källor som t.ex. IT avdelningens systeminventeringsprojekt och Upphandlingsenhetens avtalskatalog.

- I samverkan med IT-avdelningen har vi under året vid ett flertal tillfällen gjort så kallad informationsklassning av såväl befintliga som nya system med stöd av en modell framtagen av SKL som benämns KLASSA. Modellen används numera konsekvent av oss och IT.

Övriga aktiviteter:

- Under året har vi lämnat kontinuerligt stöd till FVIS-projektet. Den 24 augusti kunde projektet publicera den andra och slutliga fasen av upphandlingsunderlag för FVIS. Upphandlingen Framtidens vårdinformationsstöd genomförs gemensamt av landstingen Blekinge, Sörmland, Västerbotten samt region Västernorrland och region Örebro län.

- Vi har medverkat vid framtagningen flera nya och reviderade rutiner t.ex. reviderad rutin för registerutdrag, ny rutin för extern åtkomst av e-post/hemmakataloger, ny rutin för flyttning och borttagning av felaktigt införd journaluppgift samt en reviderad rutin för patientidentifiering.

- Arbete med ett förtydligat styrdokument kring utlämnande av handlingar främst inriktat på komplettering till följd av behov inom FoU-området har inletts.

- Vid flera tillfällen har stöd lämnats till Upphandling i såväl nya som befintliga ärenden.

- Vi har deltagit i en pilotverksamhet med en särskild grupp bildad inom Verksamhet Administration benämnd Specialistgruppen som kan fungera mycket väl som en rådgivande och stödjande instans i flera olika processer framförallt då med inriktning på informationshantering. Kompetensområden som för närvarande täcks in är arkiv, juridik, informationssäkerhet, personuppgifts-behandling, avvikelsehantering samt identitet- och behörighetsstyrning. Gruppen kan bidra med stöd i form av t.ex. granskningar och rådgivning. Stöd har också lämnats vid flera tillfällen och en ständigt ökande tillströmning av ärenden tyder på att detta är en efterfrågad verksamhet.

I revisionsplanen för året ingick en särskild granskning av IT-säkerheten vilket gav slutligen gav upphov till ett beslut om en utredning kring hur regionen ska fördjupa och förtydliga ledningssystemet för informationssäkerhet som ju är det regleringsområde IT-säkerheten ingår i.

Som en del av internkontrollen har den årliga internrevisionen av SITHS, Säker IT i Hälso- och Sjukvård genomförts. Revisionen hade en särskild inriktning på den problematiska reservkortshanteringen. Inera genomförde också under våren en extern revision av SITHS och HSA på Kramfors kommun som när det gäller SITHS utgör en del av regionens ansvarsområde.

Under året har arbetet med systematiska och regelbundna stickprovskontroller av åtkomster varje månad slumpvis tagit fram 200 patienter som fördelats till de aktuella vårdenheterna för verksamhetschefernas åtkomstgranskning.

När det gäller riktad åtkomstkontroll vilken oftast i praktiken benämns loggkontroll och leder till en så kallad ”Begäran om loggutdrag” har 56 ärenden inkommit där 43 kommit från begärande patienter, 10 kommit från verksamhetschefer för intern kontroll och 3 inkommit som en del av utredningen i IVO-ärenden.

Inget ärende med misstanke om dataintrång har registrerats under året.

För granskning av journalföring har en särskild gruppering bildats med uppdrag att för sin egen verksamhet och regionen i en regionsgemensam arbetsgrupp genomföra journalgranskningar som ett led i arbetet för ökad patientsäkerhet. Detta arbete innefattar att ta del av information i olika journal- och dokumentationssystem som regionen använder sig av inom samtliga regionens verksamheter.

2018-03-21 //Tommy Sköld, informationssäkerhetssamordnare, RVN